

Administrator's Guide

Version 8.3 | January 2014 | DOC2742A

Polycom® RealPresence® Collaboration Server (RMX) 1500/1800/2000/4000



Trademark Information

POLYCOM® and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.



This software has not achieved UC APL certification.

This document provides the latest information for security-conscious users running Version 8.3.software. The information in this document is not intended to imply that DoD or DISA certifies Polycom RMX systems.



For regulatory notices see individual Polycom® RealPresence® Collaboration Server (RMX) 1500/1800/2000/4000 Hardware Guides.

End User License Agreement

Use of this software constitutes acceptance of the terms and conditions of the Polycom® RealPresence® Collaboration Server (RMX®) 1500/1800/2000/4000 system end-user license agreements (EULA).

The EULA for your version is available on the Polycom Support page for the Polycom® RealPresence® Collaboration Server (RMX®) 1500/1800/2000/4000 system.

© 2014 Polycom, Inc. All rights reserved. Polycom, Inc. 6001 America Center Drive San Jose CA 95002 USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording). Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Contents

Overview 1
About the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Administrator's
Guide
Who Should Read This Guide?
Prerequisites
How This Guide is Organized
About the Polycom® RealPresence Collaboration Server (RMX) 1500/1800/2000/4000
System
Network Services Guidelines
IP Networks 6
ISDN Networks (Collaboration Server 1500/2000/4000)
Card Configuration Modes (Collaboration Server (RMX) 1500/2000/4000 Only) 7
Viewing the Card Configuration Mode (RMX 1500, 2000, and 4000 only)
Features Only Supported with MPMRx Cards
Workstation Requirements
Conferencing Modes Overview
AVC Conferencing
Continuous Presence (CP) Conferencing
Video Protocol Support in CP Conferences
Video Switching (VSW) Conferencing
Video Switching (VSW) Conferencing Guidelines
AVC Basic Conferencing Parameters
Supplemental Conferencing Features
SVC-based Conferencing
SVC Conferencing Guidelines
MCU Supported Resolutions for SVC Conferencing
Mixed CP and SVC Conferencing
MCU Resource Capacities for Mixed CP and SVC Conferences
Using Conference Profiles
•
Conferencing Parameters Defined in a Profile
Conferencing Capabilities in the Various Conferencing Modes

	Default Profile Settings in CP Conferencing Mode	29
	Default Profile Settings in SVC Only Conferencing Mode	31
	Default Profile Settings in a Mixed CP and SVC Conferencing Mode	32
	Viewing the List of Conference Profiles	34
	Profiles Toolbar	36
	Modifying an Existing Profile	36
	Deleting a Conference Profile	37
	Defining New Profiles	37
	Exporting and Importing Conference Profiles	38
	Guidelines for Exporting and Importing Conference Profiles	38
	Exporting Conference Profiles	38
	Exporting All Conference Profiles from an MCU	38
	Exporting Selected Conference Profiles	39
	Importing Conference Profiles	40
Dofini	ng AVC-Based Conference Profiles	12
Dellilli	Defining AVC CP Conferencing Profiles	
	•	
	Additional Information for Setting CP Profiles	
	Gathering Phase Cuidelines	
	Gathering Phase Guidelines	
	Gathering Phase Duration	
	Enabling the Gathering Phase Display	
	Overlay Layouts	
	Guidelines for using the Overlay Layouts	
	Selecting the Overlay Layouts	
	Site Names Definition	
	Guidelines	
	Site Names Display Position	
	Sending Text Messages During a Conference Using Message Overlay	
	Guidelines	
	Selecting the Chinese Font for Text Display	
	Selecting the Chinese Font	
	Defining an AVC Video Switching Conference Profile	
	H.264 High Profile Support in Video Switching Conferences	
	Minimum Threshold Line Rate System Flags	88
Defini	ng SVC and Mixed CP and SVC Conference Profiles	91
	Defining SVC Conference Profiles	91
	Defining Mixed CP and SVC Conferencing Profiles	02

Video	Protocols and Resolution Configuration for CP Conferencing	104
	Video Resolutions in AVC-based CP Conferencing	104
	Video Display with CIF, SD and HD Video Connections	104
	H.264 High Profile Support in CP Conferences	105
	H.264 High Profile Guidelines	105
	HD1080p60 Resolution Guidelines	106
	CP Conferencing with H.263 4CIF	107
	H.263 4CIF Guidelines	107
	The CP Resolution Decision Matrix	108
	Video Resource Usage	108
	H.264 Base Profile Decision Matrix	109
	H.264 High Profile Decision Matrices (MPMx/MPMRx)	112
	H.264 Base Profile and High Profile Comparison	115
	H.264 Base Profile and High Profile Comparison - Sharpness	115
	H.264 Base Profile and High Profile Comparison - Motion	122
	Default Minimum Threshold Line Rates and Resource Usage Summary	125
	Resolution Configuration for CP Conferences	126
	Guidelines	127
	Accessing the Resolution Configuration Dialog Box	127
	The Resolution Configuration Dialog Box in MPMx/MPMRx Card Configuration Modes	127
	Resolution Configuration - Basic	130
	Maximum CP Resolution Pane	130
	Resolution Configuration Pane	130
	Resolution Configuration - Detailed	131
	Sharpness and Motion	132
	Resolution Configuration Sliders	132
	Modifying the Resolution Configuration in MPMx Card Configuration Mode	134
	Flag Settings	135
	Setting the Maximum CP Resolution for Conferencing	135
	Minimum Frame Rate Threshold for SD Resolution	136
	Limiting The Maximum Negotiated Bit Rate for SD and Lower Resolutions	136
	Additional Video Resolutions in MPMx Card Configuration Mode	136
	w448p Resolution	137
	Guidelines	137
	Content	138
	Packet Loss Compensation	138
	Enabling Support of the w448p Resolution	138
	Collaboration Server System Flag Settings	139
	Additional Intermediate Video Resolutions	139

Sha	ring Content During Conferences	140
	Content Sharing Using H.239 Protocol	140
	Content Sharing Using People+Content Protocol	140
	Guidelines for Content Sharing Using People+Content Protocol	140
	SIP BFCP Content Capabilities	142
	Guidelines for Using SIP BFCP Content	142
	BFCP support in dial-out Connections	143
	BFCP support in dial-in Connections	143
	Video Transmission Methods for Sharing Content	143
	Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode	144
	Content Settings	144
	AVC CP Content Setting	144
	SVC Only and Mixed CP and SVC Content Setting	146
	Content Protocols	147
	H.263 & H.264 Auto Selection (AVC CP Conferences)	147
	H.263 (AVC CP Conferences)	147
	H.264 HD (AVC CP default)	148
	H.264 Cascade and SVC Optimized	149
	Defining Content Sharing Parameters for a Conference	151
	Enabling H.264 Cascade and SVC Optimized Content Sharing in	
	AVC CP Conferences	
	Selecting a Customized Content Rate in AVC CP Conferences	
	Guidelines for Selecting a Customized Content Rate	
	Modifying the Threshold Line Rate for HD Resolution Content	
	Sharing Content Using Multiple Content Resolutions Mode	
	Guidelines for Sharing Contents using Multiple Content Resolutions	
	Enabling Multiple Content Resolutions for Content Sharing	
	Sending Content to Legacy Endpoints (AVC Only)	
	Guidelines for Sending Content to Legacy Endpoints	
	Content Display on Legacy Endpoints	
	Interoperability with Polycom CMA and RealPresence DMA System	
	Enabling the Send Content to Legacy Endpoints Option	
	Changing the Default Layout for Displaying Content on Legacy Endpoints	
	Sending Content to Legacy Endpoints in Telepresence Mode	
	Exclusive Content Mode	
	Guidelines for Sharing Content in Exclusive Content Mode	
	Stopping a Content Session	
	Content Broadcast Control	
	Guidelines for Controlling Content Broadcast	
	Giving and Cancelling Token Ownership (AVC Participants)	1/4

Forcing Oth	ner Content Capabilities	175
Content Sh	aring via the Polycom CCS Plug-in for Microsoft Lync Clients	175
Managing N	Noisy Content Connections	176
Conten	t Display Flags	176
Implementing N	Media Encryption for Secured Conferencing	177
Media Encr	yption Guidelines	177
Mixing Enci	rypted and Non-encrypted Endpoints in one Conference	178
Direct C	Connection to the Conference	179
Connec	ction to the Entry Queue	180
Moving	from the Entry Queue to Conferences or Between Conferences	181
Record	ing Link Encryption	182
Enabling M	edia Encryption for a Conference	182
Setting	the Encryption Flags	182
Enablin	ng Encryption in the Profile	183
Enablin	ng Encryption at the Participant Level	183
Monitoring t	the Encryption Status	184
Setting Confere	ences for Telepresence Mode (AVC CP)	186
Collaboration	on Server Telepresence Mode Guidelines	186
System	Level	186
Confere	ence Level	187
Automa	atic Detection of Immersive Telepresence (ITP) Sites	187
Horizon	ntal Striping	188
Croppir	ng	188
Gatheri	ing Phase with ITP Room Systems	188
Aspect	ratio for standard endpoints	188
Skins a	ind Frames	188
RPX ar	nd OTX Video Layouts	189
Room Swite	ch Telepresence Layouts	191
Telepre	esence Display Decision Matrix	191
Guidelii	nes for Managing the Room Switch Telepresence Layouts by the MCU	192
Sending Co	ontent to Legacy Endpoints in Telepresence Conferences	193
Guidelii	nes for Sending Content to Legacy Endpoints in Telepresence Conference	es 193
Cor	ntent Display on Legacy Endpoints in Telepresence Conferences	193
Enabling Te	elepresence Mode	194
•	Telepresence Mode	
Monitor	ring Ongoing Conferences	196
Monitor	ring Participant Properties	197
Creating Mu	ultiple Cascade Links Between Telepresence Conferences	198

Guidelines for Creating Multiple Cascading Links between Conferences	198
Enabling and Using Multiple Cascade Links	199
Creating a Link Participant	201
Link Participant in the Dial Out RMX	201
Participant Link in the Dial In RMX	203
Monitoring Multiple Cascade Links	204
Disconnection Causes	204
Additional Conferencing Information	206
Video Preview (AVC Participants Only)	206
Video Preview Guidelines	206
Workstation Requirements to Display Video Preview	207
Testing your Workstation	207
Previewing the Participant Video	208
Auto Scan and Customized Polling in Video Layout (CP Conferences Only)	209
Guidelines for Using Auto Scan and Customized Polling	210
Enabling the Auto Scan and Customized Polling (CP Only Conferences)	210
Enabling the Auto Scan	210
Customized Polling	211
Packet Loss Compensation (LPR and DBA) AVC CP Conferences	212
Packet Loss	212
Causes of Packet Loss	212
Effects of Packet Loss on Conferences	212
Lost Packet Recovery	213
Lost Packet Recovery Guidelines	213
Enabling Lost Packet Recovery	213
Monitoring Lost Packet Recovery	214
Network Quality Indication (AVC Endpoints)	216
Network Quality Levels	216
Indication Threshold Values	216
Guidelines for Displaying the Network Quality icons	217
Customizing Network Quality Icon Display	217
Lecture Mode (AVC CP Only)	219
Enabling Lecture Mode	219
Selecting the Conference Lecturer	219
Enabling the Automatic Switching	221
Lecture Mode Monitoring	222
Restricting Content Broadcast to Lecturer	224
Muting Participants Except the Lecturer (AVC CP Only)	225
Guidelines for Muting all the Participants Except the Lecturer	225

	Enabling the Mute Participants Except Lecturer Option	226
	Audio Algorithm Support	227
	Audio Algorithm Support Guidelines	227
	SIP Encryption	227
	Mono	227
	Stereo	228
	Audio algorithms supported for ISDN (Collaboration Server 1500/2000/4000 only)	229
	Monitoring Participant Audio Properties	230
	Automatic Muting of Noisy Endpoints (AVC Endpoints)	232
	Guidelines for Automatically Muting Noisy Endpoints	232
	Enabling or Disabling the Automatic Muting of Noisy Endpoints	233
	Enabling or Disabling the Automatic Muting of Noisy Endpoints at the	
	Conference Level	
	Enabling or Disabling the Automatic Muting of Noisy Endpoints at the MCU Level .	
	Permanent Conference	
	Guidelines	
	Enabling a Permanent Conference	
	Closed Captions (AVC Endpoints)	
	Closed Captions Guidelines	
	Enabling Closed Captions	238
Defi	ining Cascading Conferences	239
- 0	Cascading Link Properties	
	Setting the Video Layout in Cascading conferences (CP and mixed CP and SVC)	
	Guidelines for Setting the Video Layout in Cascading Conferences	
	Flags Controlling Cascading Layouts	
	DTMF Forwarding	
	Play Tone Upon Cascading Link Connection	
	Possible Cascading Topologies	
	Basic Cascading	
		242
	-	
	Basic Cascading using IP Cascaded Link	243
	Basic Cascading using IP Cascaded Link	243 243
	Basic Cascading using IP Cascaded Link Dialing Directly to a Conference Dialing to an Entry Queue	243243243
	Basic Cascading using IP Cascaded Link Dialing Directly to a Conference Dialing to an Entry Queue Automatic Identification of the Cascading Link	243 243 243 244
	Basic Cascading using IP Cascaded Link Dialing Directly to a Conference Dialing to an Entry Queue Automatic Identification of the Cascading Link Basic Cascading using ISDN Cascaded Link	243243243244244
	Basic Cascading using IP Cascaded Link Dialing Directly to a Conference Dialing to an Entry Queue Automatic Identification of the Cascading Link Basic Cascading using ISDN Cascaded Link Network Topologies Enabling Content Sharing Over ISDN Cascaded Links	243 243 243 244 244 244
	Basic Cascading using IP Cascaded Link Dialing Directly to a Conference Dialing to an Entry Queue Automatic Identification of the Cascading Link Basic Cascading using ISDN Cascaded Link Network Topologies Enabling Content Sharing Over ISDN Cascaded Links Guidelines	243 243 243 244 244 244 245
	Basic Cascading using IP Cascaded Link Dialing Directly to a Conference Dialing to an Entry Queue Automatic Identification of the Cascading Link Basic Cascading using ISDN Cascaded Link Network Topologies Enabling Content Sharing Over ISDN Cascaded Links Guidelines Gateway to Gateway Calls via ISDN Cascading Link	243 243 243 244 244 244 245 245
	Basic Cascading using IP Cascaded Link Dialing Directly to a Conference Dialing to an Entry Queue Automatic Identification of the Cascading Link Basic Cascading using ISDN Cascaded Link Network Topologies Enabling Content Sharing Over ISDN Cascaded Links Guidelines	243 243 244 244 244 245 245 246

	Collaboration Server Configuration Enabling ISDN Cascading Links	247
	Suppression of DTMF Forwarding	252
	Star Cascading Topology	253
	Master-Slave Cascading	253
	Creating a Cascade Enabled Dial-out/Dial-in Participant Link	255
	Cascading via Entry Queue	259
	Enabling Cascading	260
	Creating the Cascade-enabled Entry Queue	260
	Creating the Dial-out Cascaded Link	262
	Enabling Cascaded Conferences without Password	264
	Monitoring Star Cascaded Conferences	264
	Creating the Dial-out Link from a Conference Running on the MGC to the Conference Running on the Collaboration Server	265
	Cascading Conferences - H.239-enabled MIH Topology	
	MIH Cascading Levels	
	Cascading Topologies	
	MIH Cascading Guidelines in CP Licensing	
	MGC to Collaboration Server Cascading	
	v	
Meet	ting Rooms	281
	Meeting Rooms List	282
	Meeting Room Toolbar & Right-click Menu	284
	Creating a New Meeting Room	285
Entry	y Queues, Ad Hoc Conferences and SIP Factories	
	Entry Queues	
	Defining a New Entry Queue	
	Listing Entry Queues	
	Modifying the EQ Properties	
	Transit Entry Queue	
	Setting a Transit Entry Queue	292
	IVR Provider Entry Queue (Shared Number Dialing)	293
	Call Flow	293
	Guidelines for setting the Entry Queue as IVR Provider	293
	Configuring the Collaboration Server as IVR Provider	293
	Using External IVR Services via the MCCF-IVR Package	295
	Call Flows	295
	Guidelines for Using External IVR Services via the MCCF-IVR Package	297
	Configuring the MCU to Support External IVR Services via the MCCF-IVR	297
	Configuring the Entry Queue to Use External IVR Services	297
	comigating and analy quous to coo antennal trick controls the trick and the control of the contr	
	SIP Factories	

	Creating SIP Factories	299
	SIP Registration & Presence for Entry Queues and SIP Factories with SIP Servers	300
	Guidelines for registering Entry Queues and SIP Factories with SIP Servers	300
	Monitoring Registration Status	301
	Ad Hoc Conferencing	301
	Gateway to Polycom® Distributed Media Application™ (DMA™) 7000 (Collaboration Server 1500/2000/4000 only)	302
Addr	ess Book	303
	Viewing the Address Book	304
	Displaying and Hiding the Group Members in the Navigation Pane	304
	Participants List Pane Information	305
	Displaying and Hiding the Address Book	
	Adding Participants from the Address Book to Conferences	
	Adding Individual Participants from the Address Book to Conferences	
	Adding a Group from the Address Book to Conferences	
	Participant Groups	
	Managing Groups in the Address Book	
	Managing the Address Book	
	Guidelines	
	Adding a Participant to the Address Book	
	Adding a New participant to the Address Book Directly	
	Substituting E.164 Number in Dial String	
	Adding a Participant from an Ongoing Conference to the Address Book	
	Modifying Participants in the Address Book	
	Deleting Participants from the Address Book	
	Copying or Moving a Participant	
	Searching the Address Book	
	Filtering the Address Book	
	Filtering Address Book Data Using a Predefined Pattern	
	Filtering Address Book Data Using a Custom Pattern	
	Clearing the Filter	
	Obtaining the Display Name from the Address Book	
	Guidelines for Obtaining the Display Name from the Address Book	
	Enabling and Disabling the Obtain Display Name from Address Book Feature	
	Importing and Exporting Address Books	
	Exporting an Address Book	
	Importing an Address Book	
	Upgrading and Downgrading Considerations (Collaboration Server 1500/2000/4000 only) .	
	Integrating the Global Address Book (GAB) of Polycom RealPresence Resource Manager (XMA) or Polycom CMA™ with the Collaboration Server	
	(Alvia) of a digoditi civia — with the collabolation server	J_C

Polycom, Inc. ix

Guidelines for integrating with the Global Address Book of Polycom RealPresence Resource Manager (XMA) or Polycom CMA™	. 326
Scheduling Reservations	328
Guidelines for Scheduling Reservations	. 328
System	. 328
Resources	. 328
Reservations	. 329
Using the Reservation Calendar	. 330
Toolbar Buttons	. 330
Reservations Views	. 331
Week View	. 331
Day View	. 331
Today View	. 332
List View	. 332
Changing the Calendar View	. 333
Scheduling Conferences Using the Reservation Calendar	. 335
Creating a New Reservation	. 335
Managing Reservations	. 341
Guidelines	. 341
Viewing and Modifying Reservations	. 341
Using the Week and Day views of the Reservations Calendar	. 341
Adjusting the Start Times of all Reservations	. 343
Deleting Reservations	. 344
Searching for Reservations using Quick Search	. 345
Operator Assistance & Participant Move	347
Operator Conferences	. 347
Operator Conference Guidelines	. 348
Defining the Components Enabling Operator Assistance	. 348
Defining a Conference IVR Service with Operator Assistance Options	. 349
Defining an Entry Queue IVR Service with Operator Assistance Options	. 351
Defining a Conference Profile for an Operator Conference	. 352
Starting an Ongoing Operator Conference	. 354
Saving an Operator Conference to a Template	. 357
Starting an Operator Conference from a Template	. 358
Monitoring Operator Conferences and Participants Requiring Assistance	. 359
Requesting Help	. 359
Participant Alerts List	. 360
Audible Alarms	. 361
Using Audible Alarms	. 361

Moving Participants Between Conferences	
Moving Participants Options	
Conference Templates	364
Guidelines	364
Using Conference Templates	365
Toolbar Buttons	366
Creating a New Conference Template	366
Creating a new Conference Template from Scratch	366
Saving an Ongoing or AVC-based CP Operator Conference as a Template .	373
Starting an Ongoing Conference From a Template	374
Starting an Operator Conference from a Template (AVC Conferencing) .	375
Scheduling a Reservation From a Conference Template	376
Deleting a Conference Template	378
Exporting and Importing Conference Templates	379
Exporting Conference Templates	379
Exporting All Conference Templates from an MCU	379
Exporting Selected Conference Templates	381
Importing Conference Templates	382
Polycom Conferencing for Microsoft Outlook®	385
Setting up the Calendaring Solution	
Calendaring Guidelines	
Creating and Connecting to a Conference	
Creating a Conference	
Connecting to a Conference	
Collaboration Server Standalone Deployment	
Collaboration Server and Polycom RealPresence DMA System Deployment	
Polycom Solution Support	395
Conference and Participant Monitoring	396
General Monitoring	
Conference Level Monitoring	
Viewing the Properties of Ongoing CP and Mixed CP and SVC Conferences	
Viewing the Properties of Ongoing SVC-based Conferences	
Monitoring of Operator Conferences and Participants Requiring Assistance	408
(CP and Mixed CP and SVC Conferences)	415
Requesting Help	
Request to Speak	
Participant Alerts List	
Participant Level Monitoring	

Polycom, Inc. xi

Viewing the Properties of Participants	419
Monitoring IP Participants	420
Monitoring SIP BFCP Content	430
Detecting SIP Endpoint Disconnection	431
Monitoring ISDN/PSTN Participants	432
Monitoring Telepresence Participant Properties	439
Recording Conferences	. 440
Creating Multiple Virtual Recording Rooms on the RSS	441
Configuring the Collaboration Server to Enable Recording	441
Defining the Recording Link	441
Enabling the Recording Features in a Conference IVR Service	443
Enabling the Recording in the Conference Profile	444
Recording Link Encryption	446
Recording Link Encryption Flag Setting	446
Recording Link Settings	447
Managing the Recording Process	448
Recording Link Layout	448
Using the Collaboration Server Web Client to Manage the Recording Process	449
Using DTMF Codes to Manage the Recording Process	450
Conference Recording with Codian IP VCR	451
Users, Connections, and Notes	452
Collaboration Server Users	
User Types	
Administrator	
Administrator Read-only	
Operator	
Chairperson	
Auditor	
Machine Account	
Listing Users	
Adding a New User	
Deleting a User	
Changing a User's Password	
Disabling a User	
Enabling a User	
Renaming a User	
Machine Account	
Guidelines for defining a machine account	
	•

Polycom, Inc. xii

	Monitoring	460
	Active Directory	460
	Connections	460
	Viewing the Connections List	460
	Notes	461
	Using Notes	461
IP Ne	etwork Services	463
	Collaboration Server IP Network Services Overview	463
	Management Network (Primary)	464
	Default IP Service (Conferencing Service)	464
	Using IPv6 Networking Addresses for Collaboration Server Internal and External Entities	165
	IPv6 Addressing Guidelines	
	Modifying the Default ID Network	
	Modifying the Default IP Network Service	
	Ethernet Settings	
	•	
	LAN Redundancy	
	Media Redundancy on RealPresence Collaboration Server (RMX) 1500	
	Media Redundancy on RealPresence Collaboration Server (RMX) 2000/4000	
	Media and Signaling Redundancy on RealPresence Collaboration Server	499
	(RMX) 1800	500
	Signaling and Management Redundancy	
	Signaling and Management Redundancy on RealPresence Collaboration Server	
	(RMX) 1500	501
	Signaling and Management Redundancy on RealPresence Collaboration Server	
	(RMX) 4000	
	Management Redundancy on RealPresence Collaboration Server (RMX) 1800	
	Configuration Requirements	
	RealPresence Collaboration Server (RMX) 1500	
	RealPresence Collaboration Server 1800	
	RealPresence Collaboration Server (RMX) 2000	
	RealPresence Collaboration Server (RMX) 4000	
	On all systems:	
	Hardware Monitor Indications	
	Network Traffic Control	
	SIP Proxy Failover With Polycom® Distributed Media Application™ (DMA™) 7000	
	RealPresence Collaboration Server (RMX) Network Port Usage	507

Polycom, Inc. xiii

Defining ISDN/PSTN Network Services	. 509
IISDN/PSTN Network Services Overview	509
Adding/Modifying ISDN/PSTN Network Services	510
Obtaining ISDN/PSTN required information	511
Modifying an ISDN/PSTN Network Service	517
Network Security	. 519
RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 4000	
RealPresence Collaboration Server 1800	519
RealPresence Collaboration Server (RMX) 2000	519
Multiple Network Services	519
Guidelines	521
Resource Allocation and Capacity	523
First Time Installation and Configuration	523
Upgrading to Multiple Services	524
Gather Network Equipment and Address Information - IP Network Services Required Information	524
RealPresence Collaboration Server (RMX) Hardware Installation	525
RealPresence Collaboration Server (RMX) 4000 Multiple Services Configuration	. 526
RealPresence Collaboration Server (RMX) 2000 Multiple Services Configuration	. 527
RealPresence Collaboration Server (RMX) 1800 Multiple Services Configuration	. 529
RealPresence Collaboration Server (RMX) 1500 Multiple Services Configuration	. 530
Collaboration Server Configuration	531
System Flags and License Settings	531
IP Network Service Definition	531
Setting a Network Service as Default	537
Ethernet Settings	538
Signaling Host IP Address and MCU Prefix in GK Indications	538
Video/Voice Port Configuration and Resolution Configuration (Collaboration Servine 1500/2000/4000 in MPMx Card Configuration Mode only)	
Conference Profile	
Gateway Profiles	
Hardware Monitor	
Signaling Monitor	541
Conferencing	541
Defining Dial Out Participants	
Reserving Video Resources for a Conference (Collaboration Server	
1500/2000/4000 only)	
Monitoring Conferences	
Resource Report	543

Polycom, Inc. xiv

Port Usage Gauges	544
NAT (Network Address Translation) Traversal	545
Deployment Architectures	545
Remote Connection Using the Internet	545
Business to Business Connections	546
FW (Firewall) NAT Keep Alive	546
System Configuration in SBC environments	547
SIP TCP Keep-Alive	548
IVR Services	549
IVR Services List	
IVR Services Toolbar	
Adding Languages	
Uploading a Message File to the Collaboration Server	
Defining a New Conference IVR Service	
Defining a New Conference IVR Service	
Change to Chairperson	
Controlling the receipt of in-band and out-of-band DTMF Codes	
Entry Queue IVR Service	
Defining a New Entry Queue IVR Service	
Setting a Conference IVR Service or Entry Queue IVR Service as the Default Service	
Modifying the Conference or Entry Queue IVR Service Properties	
Replacing the Music File	
Adding a Music File	580
Creating Audio Prompts and Video Slides	581
Recording an Audio Message	581
Creating a Welcome Video Slide	585
Inviting Participants using DTMF	586
Invite Call Flow	586
Entering Additional DTMF Codes	586
Error Handling	586
Guidelines	587
Enabling the Invite Participants using DTMF Option	587
Disabling the Invite Participant Option	590
External IVR Service Control	591
IVR Services Support with TIP Protocol	591
Guidelines for TIP Support with IVR Services	
Default IVR Prompts and Messages	592
Volume Control of IVR Messages, Roll Call and Music	596
IVR Services in TIP-Enabled Conferences	597

Polycom, Inc. xv

IVR Services in TIP-Enabled Conferences Guidelines	597
Entry Queue and Virtual Entry Queue Access	597
Configuring the Conference and Entry Queue IVR Services	597
Call Detail Record (CDR) Utility	599
The CDR File Properties	599
CDR File Formats	599
Multi-Part CDR Files	600
Enabling the Multi-Part CDR Option	601
CDR File Contents	601
Viewing, Retrieving and Archiving Conference Information	602
Viewing the Conference Records	602
Multi-part CDR File display	603
Refreshing the CDR List	604
Retrieving and Archiving Conference CDR Records	604
Gateway Calls	606
Gateway Functionality	606
Call Flows	607
IP Participants	607
Direct Dialing	607
Gateway IVR Dialing For IP Participants	610
Direct Dialing Using IP Addresses	611
Calling a SIP Endpoint in a Remote Domain	613
ISDN Participants	614
Dialing via Gateway IVR for ISDN Participants	614
Direct Dial-in to Endpoints or DMA VMR using Automatically Generated Destination Numbers	
Configuring the Gateway Components on the Collaboration Server	
Defining the IVR Service for Gateway Calls	
Defining the Conference Profile for Gateway Calls	
Defining the Gateway Profile	
System Configuration	
Displaying the Connection Information	622
Enabling PSTN dial-in using GK prefix	
Gateway Calls Redialing	
Gateway Redial Guidelines	
Redial on Wrong Number	
Disconnect on Busy	
Disconnect on No Answer	
Disconnect on Wrong Number	624

Polycom, Inc. xvi

	Monitoring Ongoing Gateway Sessions	624
	Connection Indications	624
	Gateway Session Parameters	625
	Connected Participant Parameters	626
	Direct Dialing from ISDN/PSTN Endpoint to IP Endpoint via a Meeting Room	627
	Dialing to Polycom® RealPresence DMA System	629
	Calling a RealPresence DMA Direct with Automatically Generated Destination Dial Strings	629
	Calling the RealPresence DMA via Gateway IVR	630
	Manual Dial String Entry	630
	Automatic Dial String Generation	631
	PSTN Dial-in Using GK Prefix	632
	Deploying a Polycom RMX [™] Serial Gateway S4GW	633
RMX	Manager Application	634
	Installing the RMX Manager Application	635
	Accessing or downloading the RMX Manager Installer	635
	Accessing the RMX Manager Application Installer Directly from the MCU	636
	Downloading the Installation files from Polycom Support Site	636
	Accessing the RMX Manager Installer from the Login screen	636
	Installing the RMX Manager on Your Workstation	637
	Starting the RMX Manager Application	638
	Connecting to the MCU	640
	RMX Manager Main Screen	642
	MCUs Pane	642
	Conferences Pane	644
	Collaboration Server Management	645
	List Pane	645
	Status Bar	645
	Address Book	647
	Conference Templates	647
	Adding MCUs to the MCUs List	647
	Starting a Conference	649
	Starting a Conference from the Conferences Pane	650
	Starting a Reservation	651
	Starting an Ongoing Conference or Reservation From a Template	652
	Monitoring Conferences	653
	Grouping the Participants by MCU	654
	Start Monitoring/Stop Monitoring	655
	Modifying the MCU Properties	656

Polycom, Inc. xvii

	Disconnecting an MCU	657
	Removing an MCU from the MCUs Pane	657
	Changing the RMX Manager Language	658
	Import/Export RMX Manager Configuration	658
	Installing RMX Manager in Secure Communication Mode	660
	Using an Internal Certificate Authority	665
Admi	nistration and Utilities	669
	System and Participant Alerts	669
	System Alerts	670
	Participant Alerts	672
	RMX Time	673
	Altering the clock	673
	Resource Management	675
	Resource Capacity	675
	MCU Capacities in CP Only Conferencing and SVC Only Conferencing	675
	MCU Capacities in Mixed CP and SVC Conferencing	677
	AVC Conferencing - Video Switching Resource Capacity (Collaboration Server 1500/2000/4000 Only)	678
	Resource Usage in AVC CP Conferencing	678
	AVC Conferencing - Voice	679
	Resource Capacity Modes	679
	Video/Voice Port Configuration - MPMRx	680
	Video/Voice Port Configuration - MPMx	680
	Flexible Resource Capacity Mode	680
	Configuring the Video/Voice Resources	681
	Forcing Video Resource Allocation to CIF Resolution	681
	Resource Reports	683
	Displaying the Resource Report	683
	Resource Report for Collaboration Servers 1500 and 2000/4000 with MPMx media cards	683
	Resource Reports for Collaboration Server 1800 and 2000/4000 with MPMRx media cards	685
	Resource Capacities in AVC CP, SVC and Mixed Mode Conferences in MPMx Card Configuration Mode	686
	Resource Capacities in AVC CP, SVC and Mixed Mode Conferences in MPMRx Card Configuration Mode	
	Collaboration Server 1800 Resource Capacity	
	Collaboration Server 2000/4000 Resource Capacity	
	ISDN/PSTN	
	MCU Resource Management by RealPresence Resource Manager (XMA), Polycom CN	

Polycom, Inc. xviii

and Polycom RealPresence DMA System	689
Guidelines	689
Port Usage Threshold	690
Setting the Port Usage Threshold	690
SIP Dial-in Busy Notification	691
Port Usage Gauges	692
System Information	693
SNMP (Simple Network Management Protocol)	695
MIBs (Management Information Base)	696
Traps	696
Guidelines	696
MIB Files	696
Private MIBs	696
Support for MIB-II Sections	697
The Alarm-MIB	697
H.341-MIB (H.341 – H.323)	697
Standard MIBs	697
Unified MIB	698
Traps	700
Status Trap	701
RMX MIB entities that do not generate traps	701
Defining the SNMP Parameters in the Collaboration Server	703
Hot Backup	710
Guidelines for Implementing Hot Backup	711
Enabling Hot Backup	711
Using Hot Backup Triggers	712
Guidelines for Configuring the Hot Backup Triggers	712
Configuring the Hot Backup Triggers	713
Modifications to the Master MCU Requiring System Reset	714
Audible Alarms	
Using Audible Alarms	715
Audible Alarm Permissions	715
Stop Repeating Message	715
Configuring the Audible Alarms	716
User Customization	716
Replacing the Audible Alarm File	717
Multilingual Setting	718
Customizing the Multilingual Setting	718
Banner Display and Customization	718
Guidelines	719

Polycom, Inc. xix

Non-Modifiable Banner Text	. 720
Sample 1 Banner	. 720
Sample 2 Banner	. 720
Sample 3 Banner	. 720
Sample 4 Banner	. 721
Customizing Banners	. 721
Banner Display	. 723
Login Screen Banner	. 723
Main Screen Banner	. 724
Software Management	. 725
Backup and Restore Guidelines	. 725
Using Software Management	. 725
Ping the Collaboration Server	. 727
Guidelines	. 727
Using Ping	. 727
Notification Settings	. 728
Logger Diagnostic Files	. 730
Information Collector	. 732
Standard Security Mode	. 732
Ultra Secure Mode	. 733
Network Intrusion Detection System (NIDS)	. 733
Using the Information Collector	. 733
Step 1: Creating the Information Collector Compressed File	. 733
Step 2: Saving the Compressed File	. 735
Step 3: Viewing the Compressed File	. 735
Auditor	. 735
Auditor Files	. 736
Retrieving Auditor Files	. 736
Auditor File Viewer	. 738
Audit Events	. 741
Alerts and Faults	. 741
Transactions	. 742
ActiveX Bypass	. 744
Installing ActiveX	. 744
Resetting the Collaboration Server	. 745
	. 745
System Configuration Flags	746
Modifying System Flags	. 746
Manually Adding and Deleting System Flags	. 763

Polycom, Inc. xx

Manually Adding Flags to the CS_MODULE_PARAMETERS Tab	789
Deleting a Flag	791
Auto Layout Configuration	791
Customizing the Default Auto Layout	791
LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values	793
CS_ENABLE_EPC Flag	794
Automatic Password Generation Flags	794
Guidelines	795
Enabling the Automatic Generation of Passwords	795
Flags Specific to Maximum Security Environments - Ultra Secure Mode	797
Ultra Secure Mode Flag	797
Ultra Secure Mode	
Enabling Ultra Secure Mode	
ULTRA_SECURE_MODE System Flag	
Guidelines	798
System Flags affected by Ultra Secure Mode	800
Certificate Management	802
(PKI) Public Key Infrastructure	802
Adding Certificates to the Certificate Repository	803
Trusted Certificates	804
Personal Certificates	807
Certificate Validation	809
CRL (Certificate Revocation List)	810
Adding a CRL	810
Removing a CRL	812
Certificate Revocation	812
Self-signed Certificate	814
Self-signed Certificate Creation	814
SIP TCP Keep-Alive	815
Keep Alive Frequency	816
User and Connection Management	817
Managing the System Users	817
User Types	817
Disabling/Enabling Users	818
Renaming Users	818
Disabling Inactive Users	818
Managing the User Login Process	818
Implementing Strong Passwords	818
Implementing Password Re-Use / History Rules	820

Polycom, Inc. xxi

Defining Password Aging	820
Maximum Repeating Characters	820
Defining Password Change Frequency	821
Forcing Password Change	821
Temporary User Lockout	821
User Lockout	821
User Login Record	822
Controlling User Sessions	822
Management Sessions per System	822
Sessions per User	823
Connection Timeout	823
Session Timeout	823
Erase Session History After Logout	823
Banner Display and Customization	823
Guidelines for Customizing the Login Page Banner	824
Non-Modifiable Banner Text	824
Sample 1 Banner	824
Sample 2 Banner	825
Sample 3 Banner	825
Sample 4 Banner	826
Customizing Banners	826
Banner Display	828
Login Screen Banner	828
Main Screen Banner	829
Securing an External Database	829
MS Active Directory Integration	830
Directory and Database Options	830
Ultra Secure Mode	830
Standard Security Mode	830
Guidelines	
Enabling Active Directory Integration	831
Restoring the RealPresence® Collaboration Server (RMX®) 1500/2000/4000 Using the USB	
AUDD (AUS)	
MLPP (Multi Level Precedence and Preemption)	
Enabling Precedence	
SIP Message	
Dial-in calls	
Dial-out calls	
Precedence Level Change	
Configuring and Modifying Precedence Domains and DSCP Values	839

Polycom, Inc. xxii

System Flags	840
Monitoring Precedence Level	840
IEEE 802.1X Authentication	841
Certificate Repository	841
Enabling and Configuring 802.1X Authentication	842
System Flags	843
Disabling 802.1X Authentication	844
Ethernet Monitoring	844
White List Access	844
Guidelines	844
Enabling, Disabling and Modifying the White List	845
Alternative Network Address Types (ANAT)	847
Guidelines	847
System Flag	847
BFCP Over UDP – AS-SIP Content	848
Guidelines	848
Enabling AS-SIP Content	
System Flag	850
Internet Control Message Protocol (ICMP)	
Guidelines	
System Flag: ENABLE_ACCEPTING_ICMP_REDIRECT	
System Flag: ENABLE_SENDING_ICMP_DESTINATION_UNREACHABLE	
Password Encryption	
Upgrade / Downgrade Guidelines	
Non-hashed Passwords	
Self-signed Certificate Creation	
Media Encryption and Authentication	
System Flag	855
Collaboration Server Hardware Monitoring	857
Viewing the Status of the Hardware Components	
HW Monitor Pane Toolbar	
Viewing the Properties of RealPresence Collaboration Server (RMX) 1500	000
Hardware Components	859
Viewing the Properties of RealPresence Collaboration Server 1800 Hardware Components	866
Resetting the RMX 1800 DSP cards	872
Temperature Thresholds	873
Viewing the Properties of RealPresence Collaboration Server (RMX) 2000	
Hardware Components	
To View the Supporting Hardware Components Properties:	879

Polycom, Inc. xxiii

Viewing the Properties of RealPresence Collaboration Server (RMX) 4000 Hardware Components	882
To View the Supporting Hardware Components Properties:	
Diagnostic Mode (RealPresence Collaboration Server (RMX) 1500/2000/4000)	
Connecting to the Shelf Management Server:	
Performing Basic Mode Diagnostics	
Performing Advanced Mode Diagnostics	
Diagnostics Monitoring	
MCU Monitor	
Cards Monitor	903
Error Buffer	904
Temperature Thresholds	904
Collaboration Server RTM-IP 1500/RTM-IP/RTM IP 4000 Card Properties	905
CNTL Card Properties	906
MPMx Card Properties	907
endix A - Disconnection Causes	909
IP Disconnection Causes	
ISDN Disconnection Causes	
	040
endix B - Active Alarms	919
endix B - Active Alarms	
endix C - CDR Fields, Unformatted File	931
	931
pendix C - CDR Fields, Unformatted File	931 932
Pendix C - CDR Fields, Unformatted File	931 932 933
The Conference Summary Record Event Records Standard Event Record Fields	931 932 933 933
The Conference Summary Record Event Records Standard Event Record Fields Event Types	931 932 933 933 934 939
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields	931 932 933 933 934 939
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server	931 932 933 934 939 966
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server	931 932 933 934 939 966 969
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server Dendix D - Ad Hoc Conferencing and External Database Authentication Ad Hoc Conferencing without Authentication	931 932 933 934 939 966 969 970
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server pendix D - Ad Hoc Conferencing and External Database Authentication Ad Hoc Conferencing without Authentication Ad Hoc Conferencing with Authentication	931 932 933 934 939 966 969 970
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server Dendix D - Ad Hoc Conferencing and External Database Authentication Ad Hoc Conferencing without Authentication	931 933 933 934 939 966 969 970 971
Pendix C - CDR Fields, Unformatted File The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server Pendix D - Ad Hoc Conferencing and External Database Authentication Ad Hoc Conferencing without Authentication Ad Hoc Conferencing with Authentication Entry Queue Level - Conference Initiation Validation with an External Database	931 932 933 934 939 966 969 970 971 972
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server Pendix D - Ad Hoc Conferencing and External Database Authentication Ad Hoc Conferencing without Authentication Ad Hoc Conferencing with Authentication Entry Queue Level - Conference Initiation Validation with an External Database Application	931 932 933 934 939 966 969 970 971 972 973
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server Pendix D - Ad Hoc Conferencing and External Database Authentication Ad Hoc Conferencing without Authentication Ad Hoc Conferencing with Authentication Entry Queue Level - Conference Initiation Validation with an External Database Application Conference Access with External Database Authentication	931 932 933 934 939 966 969 970 971 972 973 974
The Conference Summary Record Event Records Standard Event Record Fields Event Types Event Specific Fields Disconnection Cause Values MGC Manager Events that are not Supported by the Collaboration Server sendix D - Ad Hoc Conferencing and External Database Authentication Ad Hoc Conferencing without Authentication Ad Hoc Conferencing with Authentication Entry Queue Level - Conference Initiation Validation with an External Database Application Conference Access with External Database Authentication Conference Access Validation - All Participants (Always)	931 932 933 934 939 966 969 970 971 973 975

Polycom, Inc. xxiv

	Authentication Settings	977
	MCU Configuration to Communicate with an External Database Application	977
	Enabling External Database Validation for Starting New Ongoing Conferences	978
	Enabling External Database Validation for Conferences Access	979
Appen	dix E - Participant Properties Advanced Channel Information	981
Appen	dix F- Secure Communication Mode	984
(Certificate Configuration and Management	984
	Certificate Template Requirements	985
	Certificate Requirements	985
	Configure Certificate Management	985
5	Switching to Secure Mode	985
	Purchasing and Installing a Certificate	986
	Creating/Modifying System Flags	986
	Enabling Secure Communication Mode	986
	Alternate Management Network	988
F	Restoring Defaults	988
∆nnen	dix G - Configuring Direct Connections to the Collaboration Server	989
• •	Management Network (Primary)	
	Alternate Management Network	
•	Configuring the Workstation	
	Connecting to the Management Network	
	Connecting to the Alternate Management Network	
	Connecting to the Collaboration Server via Modem	
	Procedure 1: Install the RMX Manager	
	Procedure 2: Configure the Modem	
	Procedure 3: Create a Dial-up Connection	
	Procedure 4: Connect to the Collaboration Server	
Appen	dix H - Integration Into Microsoft Environments 1	002
	_	1002
	Conferencing Entities Presence	
	Multiple Networks	
	Guidelines	
	Interactive Connectivity Establishment (ICE)	
	ICE Guidelines	
	Connecting to the Collaboration Server in ICE Environment	
	Dialing Methods	

Polycom, Inc. xxv

Integrating the Collaboration Server into the Microsoft Office Communications Server Environment	1007
Setting the Matched URI Dialing Method	1007
Configuring the Office Communications Server for Collaboration Server Systems	1008
Setting the Trusted Host for Collaboration Server in the Office Communications Server	1008
Setting the Static Route for Collaboration Server in the OCS	1010
Setting the Static Route & Trusted Host for Collaboration Server in the	1010
Load Balancer Server (Optional)	1012
Configuring the Collaboration Server System	
Dialing to an Entry Queue, Meeting Room or Conference Using the Matched URI Method	1013
Setting the Numerical Dialing Method	1014
Setting the Numerical Dialing for Collaboration Server Meeting Rooms	
Optional. Removing the Collaboration Server from the Host Authorization List	
·	1015
· · · · · · · · · · · · · · · · · · ·	1016
Configuring Office Communicator Users for Enterprise Voice	
Starting a Conferencing Call from the MOC	
Setting Simultaneous Numerical Dialing and Matched URI Routing	1023
PFX Method - Creating the Security (TLS) Certificate in the OCS and Exporting the Certificate to the Collaboration Server Workstation	1024
Retrieving the Certificate from the OCS to be sent to the Collaboration Server Workstation	1029
Optional. Creating the Certificate Password File (certPassword.txt)	1031
Supporting Remote and Federated Users in Office Communications Server ICE	
Environment	1032
Creating an Active Directory Account for the Collaboration Server	
Enabling the Collaboration Server User Account for Office Communication Server	
Configure the Collaboration Server for ICE dialing	1035
Collaboration Server Integration into the Microsoft Lync Server 2010 and	4005
Lync Server 2013 Environments	
Configuring the Polycom-Microsoft Solution	
Call Admission Control (CAC)	
FEC Support	
Media Over TCP	
Network Error Recovery	
SIP Dialog Recovery	1037
Content Sharing via Polycom CSS (Content Sharing Suite) Plug-in for Lync Clients	
Configuring the Collaboration Server for Microsoft Integration	

Polycom, Inc. xxvi

Modify the Collaboration Server Management Network Service to Include the DNS Server	1038
Defining a SIP Network Service in the Collaboration Server and Installing the Security Certificate	1039
The Security Certificate	1039
Configuring the Collaboration Server IP Network Service	1040
Collaboration Server System Flag Configuration	1048
Enabling the Microsoft Environment	1048
Microsoft RTV Video Protocol Support in CP Conferences	1050
Guidelines	1050
Participant Settings	1051
Monitoring RTV	1053
Controlling Resource Allocations for Lync Clients Using RTV Video Protocol	1053
Threshold HD Flag Settings using the RTV Video Protocol	1055
Sharing Content via the Polycom CSS Plug-in for Lync Clients	1056
Guidelines	1056
Configuring the MCU for Content Sharing via the Polycom CSS Plug-in	1056
Setting the System Flag	1057
Conference Profile Settings	1057
Monitoring the Participant connection	1057
Adding Presence to Conferencing Entities in the Buddy List	1060
Guidelines	1061
Enabling the Registration of the Conferencing Entities	1062
Creating an Active Directory Account for the Conferencing Entity	1062
Enabling the Conferencing Entity User Account for Office Communication Server of Lync Server	
Defining the Microsoft SIP Server in the IP Network Service	
Enabling Registration in the Conference Profile	
Verifying the Collaboration Server Conferencing Entity Routing Name and Profile	
Monitoring the Registration Status of a Conferencing Entity in the Collaboration Server Web Client or RMX Manager Application	1067
Conferencing Entity List	1067
Conferencing Entity Properties	
Collaboration Server Configuration for CAC Implementation	
Conferencing Behavior	
Monitoring Participant Connections	1071
Connecting a Collaboration Server Meeting Room to a Microsoft AV-MCU Conference	1072
Configuring the Collaboration Server for Federated (ICE) Dialing	1073
Monitoring the Connection to the STUN and Relay Servers in the ICE Environment	1076
Monitoring the Participant Connection in ICE Environment	
ACTIVE ATOMICS AND TRUBICSHOUTHURS	1010

Polycom, Inc. xxvii

	Active Alarms	1078
	ICE Active Alarms	1079
	Troubleshooting	1081
	Known Issues	1081
	Polycom Solution Support	1081
Append	ix I - Polycom Open Collaboration Network (POCN)	. 1083
• •	ollaboration With Cisco's Telepresence Interoperability Protocol (TIP)	
	eployment Architectures	
	Single Company Model - Polycom and Cisco Infrastructure	1084
	Call Flows	1088
	Multipoint call with DMA	1088
	Multipoint call without DMA	1089
	Company to Company Models Using a Service Provider	1090
	Model 1	1090
	Call Flow	1092
	Multipoint call via Service Provider - Model 1	1092
	Multipoint call via Service Provider - Model 2	1093
	Call Flow	1095
	Multipoint call via Service Provider - Model 2	1095
Ad	dministration	1096
	Gatekeepers	1096
	Standalone Polycom CMA/DMA System as a Gatekeeper	1096
	Standalone Cisco IOS Gatekeeper	1096
	Neighbored Cisco IOS and Polycom CMA/DMA Gatekeepers	1096
	DMA	1096
	CUCM	1096
Co	onfiguring the Cisco and Polycom Equipment	1097
	Cisco Equipment	1097
	CUCM	1097
	IOS Gatekeeper	1097
	IOS and CMA Gatekeepers (Neighbored)	1097
	Polycom Equipment	1097
	Configuring the Collaboration Server	1098
	Configuring Entry Queues and IVR Services	1099
	Guidelines	1100
	Content	1100
	Procedure 1: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag	1101
	Procedure 2: Configuring Collaboration Server to statically route outbound	
	SIP calls to DMA or CUCM	1102

Polycom, Inc. xxviii

	Procedure 3: Configuring the Collaboration Server's H.323 Network Service to register with CMA gatekeeper	1103
	Procedure 4: Configuring a TIP Enabled Profile on the Collaboration Server	
	Content Sharing Behavior	
	Procedure 5: Configuring an Ad Hoc Entry Queue on the Collaboration Server if DMA is not used	
	Procedure 6: Configuring a Meeting Room on the Collaboration Server	
	Procedure 7: Configuring Participant Properties for dial out calls	
	Collaboration with Microsoft and Cisco	
	Deployment Architecture	
	Call Flow	
	Multipoint Calls using DMA	
	Administration	
	DMA	
	Microsoft Lync Server	1116
	CUCM	
	Solution Interoperability Table	
	TIP Layout Support & Resource Usage	
	Supported TIP Resolutions and Resource Allocation	
	Supported Resolutions	1118
	Resource Allocation	1118
	Configuring the Microsoft, Cisco and Polycom Components	1119
	Content Sharing Behavior	1124
	Encryption	1125
	Guidelines	1126
	Resolution Configuration	1129
	Endpoints	1130
	Content	1130
	Operations During Ongoing Conferences	1131
	Monitoring	1131
	CTS Participants	1131
	Lync Participants (RTV)	1133
	Known Limitations	1134
Appe	ndix J - Restoring Defaults	1136
	Standard Restore	1136
	Comprehensive Restore	1136
	Restoring Factory Defaults	1137
	USB Restore	1139
	Recovery Operations Performed Using a USB Device	1140
	Recovery Options	1140

Polycom, Inc. xxix

	Comprehensive Restore to Factory Defaults 1	141
	Performing a Comprehensive Restore to Factory Defaults 1	141
	Emergency CRL (Certificate Revocation List) Update	147
Appendi	ix K - SIP RFC Support1	152
Appendi	ix L - Homologation for Brazil	154
Н.:	323 & SIP Protocol Flag Options	154
	H.323 & SIP Flag Settings 1	154
	Flag name: SIP_TIMERS_SET_INDEX	154
	Flag name: H323_TIMERS_SET_INDEX	155
	Flag name: DISABLE_DUMMY_REGISTRATION	155

Polycom, Inc. xxx

Overview

About the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Administrator's Guide



The product names Polycom® RealPresence® Collaboration Server 1500, 1800, 2000, 4000 and RMX® 1500, 1800, 2000, 4000 are used interchangeably throughout this document.

The Polycom® RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Administrator's Guide provides instructions for configuring, deploying, and administering Polycom Multipoint Control Units (MCUs) for video conferencing. This guide will help you understand the Polycom video conferencing components, and provides descriptions of all available conferencing features.



The following features are not supported with Collaboration Server 1800:

- ISDN/PSTN connections
- · Video Switching Conferences
- Gateway Calls
- · Ultra Secure Mode

Any reference to these features relates to the RealPresence® Collaboration Server 1500/2000/4000.

This guide will help you perform the following tasks:

- Customize the Collaboration Server conferencing entities such as conference Profiles, IVR Services, Meeting Rooms, Entry Queues, etc., to your organization's needs (optional).
- Define Collaboration Server Users. Further customize the Collaboration Server IP Network Settings for IPv6 environments.
- In collaboration Server 1500/2000/4000 only, further customize the Collaboration Server Network Settings for ISDN networks and IP networks for Ultra Secure Mode environments. Advanced conference Management
- Define video protocols and resolution configuration for CP conferencing
- Optional. Configure Templates, the Address Book and schedule Reservations.
- Record Conferences
- Configure the Collaboration Server to support special call flows and conferencing requirements, such as Cascading Conferences.
- In the Collaboration Server 1500/2000/4000, configure the Collaboration Server to act as a gateway and manage gateway calls.

- Configure the Collaboration Server to support Polycom third party and partner environments such as Microsoft, IBM, Cisco, Avaya, Broadsoft and Siemens.
- Configure the Collaboration Server for special applications and needs by setting various system flags.
- Manage and troubleshoot the Collaboration Server's performance.

The Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide provides description of basic conferencing operations. It will help you perform the following tasks:

- Unpack the Collaboration Server system and install it on a rack.
- Connect the required cables to the Collaboration Server.
- Perform basic configuration procedures.
- Start a new conference and connect participants/endpoints to it.
- Monitor ongoing conferences
- Perform basic operations and monitoring tasks

The RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide for Maximum Security Environments provides a deployment methodology for system administrators implementing Maximum Security Environments.

Who Should Read This Guide?

System administrators and network engineers should read this guide to learn how to properly set up Polycom Collaboration Server systems. This guide describes administration-level tasks.

For detailed description of first time installation and configuration, description of the Collaboration Server (RMX) Web Client, and basic operation of your Collaboration Server system, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide.*

Prerequisites

This guide assumes the user has the following knowledge:

- Familiarity with Windows® XP or Windows 7 operating systems and interface.
- Familiarity with Microsoft® Internet Explorer® Version 7, 8 or 9.
- Basic knowledge of video conferencing concepts and terminology.

How This Guide is Organized

The following typographic conventions are used in this guide to distinguish types of in-text information.

Typographic Conventions

Convention	Description
Bold	Highlights interface items such as menus, soft keys, flag names, and directories. Also used to represent menu selections and text entry to the phone.
Italics	Used to emphasize text, to show example values or inputs, file names and to show titles of reference documents available from the Polycom Support Web site and other reference sites.

Typographic Conventions

Convention	Description
Underlined Blue	Used for URL links to external Web pages or documents. If you click on text in this style, you will be linked to an external document or Web page.
Blue Text	Used for cross referenced page numbers in the same or other chapters or documents. If you click on blue text, you will be taken to the referenced section. Also used for cross references. If you click the italic cross reference text, you will be taken to the referenced section.
<variable name=""></variable>	Indicates a variable for which you must enter information specific to your installation, endpoint, or network. For example, when you see <ip address="">, enter the IP address of the described device.</ip>
>	Indicates that you need to select an item from a menu. For example, Administration > System Information indicates that you need to select System Information from the Administration menu.

About the Polycom® RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 System

The RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 system is a high performance, scalable, IP-network (H.323 and SIP) and ISDN/PSTN (Collaboration Server 1500/2000/4000) MCU that provides feature-rich and easy-to-use multipoint voice and video conferencing.

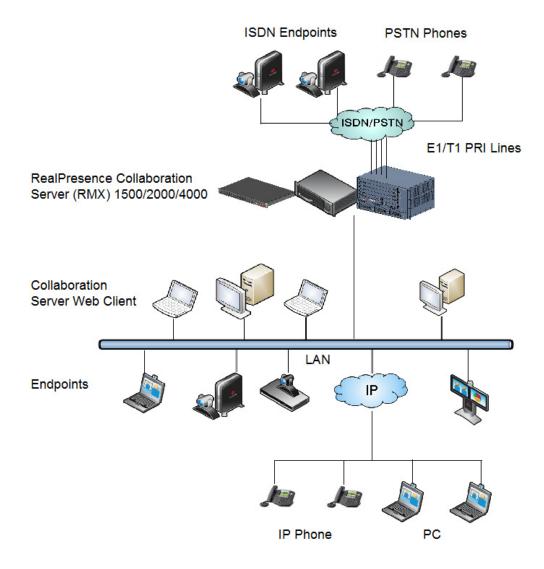
The Collaboration Server 1500/2000/4000 meets International Telecommunication Union - Telecommunication Standardization Sector, (ITU-T, formerly CCITT) standards for multipoint multimedia bridging devices, and meets ETSI standards for telecommunication products. In addition, it has been designed in compliance with IETF (Internet Engineering Task Force).

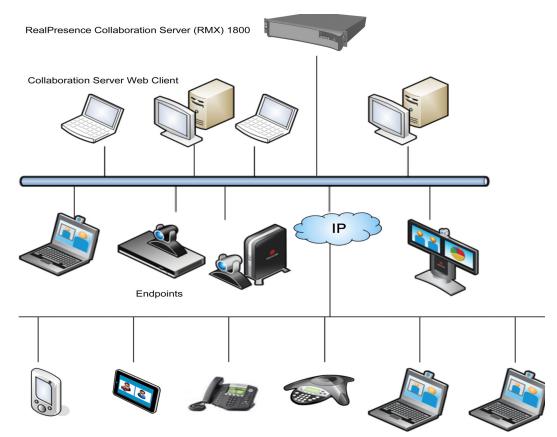
The MCU can be used as a standalone device to run voice and video conferences or it can be used as part of a solution provided by Polycom. This solution may include the following components:

- Polycom® RSS™ 4000 provides one-touch recording and secure playback on telepresence and video conferencing systems, tablets and smartphones, or from your Web browser.
- Polycom® Distributed Media Application™ (DMA™) system provides call control and MCU virtualization with carrier-grade redundancy, resiliency and scalability.
- Polycom Real Presence Resource Manager centrally manages, monitors and delivers Cloud based Video as a Service (VaaS) and enterprise video collaboration.
- Polycom® RealPresence® Access Director™ (RPAD) removes communication barriers and enables internal and external teams to collaborate more easily and effectively over video.

The following diagram describes the multipoint video conferencing configuration with the Collaboration Server as a standalone system.

Multipoint Video Conferencing using a RealPresence Collaboration Server (RMX) 1500/2000/4000





Multipoint Video Conferencing using a RealPresence Collaboration Server 1800

The RealPresence Collaboration Server system can be controlled via the LAN, by the Collaboration Server Web Client application, using Internet Explorer installed on the user's workstation or the RMX Manager application. The RMX Manager can control several MCU units. For more information about the RMX Manager, see RMX Manager Application.

In the RealPresence Collaboration Server (RMX) 1500/2000, MCU management and IP conferencing are performed via a single LAN port. The networks can be separated in Maximum Security Environments.

In the RealPresence Collaboration Server (RMX) 4000/1800, MCU management and IP conferencing are performed via two different LAN ports. The networks can be separated in Maximum Security Environments. Management and IP Service can be combined in one LAN port or separate to different ports.

The RealPresence Collaboration Server 1800 system is an IP Only MCU and does not support ISDN connections.

RealPresence Collaboration Server (RMX) 1500 supports one ISDN card with up to 4 E1/T1 PRI lines.

RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000 support a maximum of two RTM ISDN cards, each providing connection for up to either 7 E1 or 9 T1 PRI lines.

On RealPresence Collaboration Server (RMX) 1500/2000/4000, E1 and T1 connections cannot be used simultaneously.

Network Services Guidelines

IP Networks

In the Collaboration Server 1500/2000 system management and IP conferencing are performed via a single LAN port.

In the Collaboration Server 1800 system management and IP conferencing are performed on separate LAN ports.

Management uses LAN1 and IP network Services use LAN2. When enabling multiple services, management and the IP network service (1) share LAN1, the second IP network service (2) uses LAN2. The networks can be separated in Maximum Security Environments (Collaboration Server 1500/2000/4000).

In the RealPresence Collaboration Server (RMX) 4000, system management and IP conferencing are performed via two different LAN ports. The networks can be separated in Maximum Security Environments (Collaboration Server 1500/2000/4000).

ISDN Networks (Collaboration Server 1500/2000/4000)

RealPresence Collaboration Server (RMX) 1500 supports one ISDN card with up to 4 E1/T1 PRI lines.

RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000 support a maximum of two RTM ISDN cards, each providing connection for up to either 7 E1 or 9 T1 PRI lines.

On the RealPresence Collaboration Server (RMX) 1500/2000/4000, E1 and T1 connections cannot be used simultaneously.

For more detailed information about Collaboration Server abilities, see the *RealPresence Collaboration Server (RMX) Hardware Guides, Hardware Description*.

Card Configuration Modes (Collaboration Server (RMX) 1500/2000/4000 Only)

The media card installed in the system determines the **Card Configuration Mode**. The **Card Configuration Mode** represents different generations of the media card. Each new generation provides additional functionality, higher video resolutions and higher resource capacity.

Only one Media Card **type** can be installed in any Collaboration Server, which sets the **Card Configuration Mode** for that Collaboration Server:

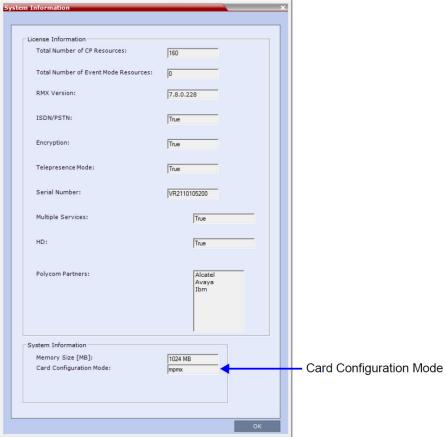
- MPMx Card Configuration Mode Supported from Version 7.0, with MPMx cards installed in the RealPresence Collaboration Server (RMX) 1500, RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000.
- MPMRx Mode Supported from Version 8.3, with MPMRx cards installed in the RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000.

Viewing the Card Configuration Mode (RMX 1500, 2000, and 4000 only)

The Card Configuration Mode is determined according to the installed media card.

The **Licensing Mode** and the **Card Configuration Mode** for your MCU can be viewed in the **System Information** dialog box (go to **Administration > System Information**).

In the example shown here, the Collaboration Server Licensing Mode is CP Licensing, and the Card Configuration Mode is MPMx.



Features Supported with MPMx/MPMRx Cards.

The following table lists the Collaboration Server features that are supported with MPMx/MPMRx cards. .

Features Supported with MPMx/MPMRx Card Configuration Modes

Feature Name	Description
Scalable Video Coding (SVC)	Scalable Video Coding (SVC) Conferencing, based on the SVC video protocol and SAC audio protocol.
	SVC Conferencing offers high resolution video conferencing with low end-to-end latency, improved Error Resiliency and higher system capacities.
H.264 High Profile Support	The H.264 High Profile improves video quality and can reduce bandwidth requirements for video conferencing transmissions by up to 50%. Supported in IP and ISDN calls.
Support of Symmetric HD Resolutions	Support of symmetric HD video resolutions HD 1080p30 and HD 720p60.
w448 Resolution support	Improves interoperability with Tandberg MXP 990/3000 endpoints providing these endpoints the resolution of W448p (768x448 pixels) at 25fps.

Features Supported with MPMx/MPMRx Card Configuration Modes

Feature Name	Description	
Content at HD1080p Resolution	With MPMRx Content is supported at HD1080p resolution at 30 fps and 60 fps. With MPMx Content is supported at HD1080p15.	
HD H.264 Content and H.264 Content for Cascading links	Enables conference participants to receive higher quality Content in both standard conferences and cascaded conferences.	
Site Names	Additional controls over the display of site names in the conference Profile.	
Interactive Video Forcing	Participants in ongoing conferences can be interactively forced to a Video Window in the conference layout by using Drag and Drop.	
Video Preview	H.264 High Profile is supported with Video Preview.	
Recording indication	A Recording Indication can be displayed to all conference participants informing them that the conference is being recorded.	
Network Quality Indication	A Network Quality Indicator is displayed for each participant in the CP layout indicating the quality of the participants' video channels.	
Auto scan and Customized Polling	A single cell in the conference layout is used to cycle the display of participants that are not in the conference layout. The order of the cyclic display can be predefined.	
SirenLPR	Prevents audio degradation and maintains high audio (CD) quality if packet loss occurs.	
Speaker Change Threshold	The option to configure the amount of time a participant must speak continuously until becoming the speaker.	
Integration with Cisco Telepresence Systems (CTS)	The MCU natively inter-operate with Cisco TelePresence Systems and Polycom TelePresence and vide conferencing endpoints, ensuring optimum quality multi-screen, multipoint calls.	
POCN - Collaboration with Microsoft and Cisco in the same environment	The POCN solution, enables Polycom, Microsoft and Cisco users, each within their own environment, to participate in the same conference running on a Collaboration Server.	
Additional Chinese Font Types	Additional Chinese fonts may be selected for several features when using the Collaboration Server in Chinese.	
Support for Microsoft Protocols	, algorithms and workflows	
RTV Video Protocol	Microsoft RTV Video protocol is supported.	
RTV B-Frame Support	B-frame encoding and decoding are supported to enhance the viewing experience of Microsoft Lync clients. It provides higher video quality at the same bit-rate with better scalability on the decoder side.	
Conferencing Entities Presence in Microsoft Office Communications Server Client or Lync Server Client	Registration & Presence enables the OCS or LYNC client users to see the availability status (Available, Busy or Offline) of Meeting Rooms, Entry Queues and SIP Factories and connect to them directly from the buddy list.	

Features Supported with MPMx/MPMRx Card Configuration Modes

Feature Name	Description
Cascading between Collaboration Server Meeting room / Microsoft A/V MCU	Microsoft Lync users can connect a <i>Collaboration Server</i> Meeting Room to a conference running on the Microsoft A/V MCU.
FEC Support	Support of Microsoft RTV FEC (Forward Error Correction) that controls and correct packet loss when receiving and sending video streams using the Microsoft Lync Server 2010.
ICE Over TCP	Enables the automatic usage of the ICE connection through the TCP port instead of UDP when the UDP port in the firewall is blocked.
Media Over TCP	Media is automatically transmitted using TCP when UDP, the default transport protocol, is not available.
Error Recovery	The Collaboration Server can automatically recover from short duration network errors (5 seconds), enabling calls in Microsoft Lync to continue video or audio conferences without disconnecting.

Features Only Supported with MPMRx Cards

The following table lists the Collaboration Server features that are only supported with MPMRx cards. (This applies to RMX 1500, 2000, and 4000 only.)

Features Only Supported with MPMRx Card Configuration Mode

Feature Name	Description	
HD1080p60 Symmetric	HD1080p60 Resolution is symmetric	
HD1080p30/60 Content	Content is supported at resolutions of HD1080p30 and HD1080p60 in both H.264 Base and High Profiles. An additional check box H.264 High Profile and additional rate values in the Content Rate drop-down menu have been added to the Video Quality dialog box.	
6Mbps supported	The RealPresence Collaboration Server (RMX) 1800 supports AVC-CP conferences at a line rates up to and including 6Mbps.	
System Flag	A new System Flag: LIMIT_SD_AND_CIF_BW_MPMRX, when added to system.cfg and set to YES (default), limits the maximum negotiated and opened bit rate for resolutions equal or lower than SD to 1Mbps. When set to NO no limitation is applicable to SD and CIF bit rates.	

Workstation Requirements

The RMXWeb Client and RMX Manager applications can be installed in an environment that meets the following requirements:

- Minimum Hardware Intel® Pentium® III, 1 GHz or higher, 1024 MB RAM, 500 MB free disk space.
- Workstation Operating System Microsoft® Windows® XP, Windows® 7, and Windows® 8.
- Network Card 10/100/1000 Mbps.

- Web Browser Microsoft® Internet Explorer® Version 7, 8, 9, and 10.
- Collaboration Server Web client and RMX Manager are optimized for display at a resolution of 1280 x 800 pixels and a magnification of 100%

The following table lists the environments (Web Browsers and Operating Systems) with which the *Collaboration Server Web Client* and *RMX Manager* applications are supported.

Collaboration Server Wen Client/RMX Manager Environment Interoperability Table

Web Browser	Operating System	
Internet Explorer 7	Windows Vista™	
	Windows 7	
Internet Explorer 8	Windows 7	
Internet Explorer 9	Windows 7 and Windows 8	
Internet Explorer 10*	Windows 8	



* Internet Explorer 10 has been tested on the RMX 1800. If for any reason it fails to run, right-click the IE icon and select **Run As Admin**.

.Net Framework 3.5 SP1 is required and installed automatically.

Internet Explorer must be enabled to allow running Signed ActiveX. If ActiveX installation is blocked, see the ActiveX Bypass .



Collaboration Server Web Client does not support larger Windows text or font sizes. It is recommended to set the text size to 100% (default) or Normal in the Display settings in Windows Control Panel on all workstations. Otherwise, some dialog boxes might not appear properly aligned. To change the text size, select **Control Panel>Display**. For Windows XP, click the **Appearance** tab, select **Normal** for the Font size and click **OK**. For Windows 7, click the **Smaller - 100**% option and click **OK**.



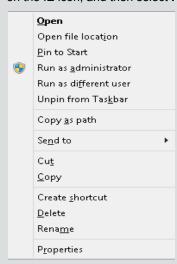
When installing the Collaboration Server Web Client, Windows Explorer **>Internet Options> Security Settings** must be set to **Medium** or less.



It is not recommended to run RMX Web Client and Polycom CMAD applications simultaneously on the same workstation.



If you have problems getting the Collaboration Server Web Client to work with Windows 8, it is recommended to run Internet Explorer as an administrator by holding the shift key and right-clicking on the IE icon, and then select **Run as Administrator**.



For Windows 7[™] Security Settings, see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, Windows 7[™] Security Settings.

For Internet Explorer 8 configuration, see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, Windows 7™ Security Settings.

Conferencing Modes Overview

The MCU system offers the following types of conferences (Conferencing Modes), based on the video protocol and the video display during the conference:

- AVC-based Conferencing CP Only (Video Transcoding)
- AVC-based Conferencing Video Switching (Collaboration Server (RMX) 1500/2000/4000 only)
- SVC-based Conferencing (Media Relay) SVC Only
- Mixed AVC and SVC Conferencing CP and SVC

AVC Conferencing

AVC-based Conferences allow endpoints that support AVC video to connect to these conferences. AVC (Advanced Video Coding) video refers to the H.264 video protocols used to send and receive video. On the Collaboration Server system it also includes all the standard video protocols such as H.261, H.263, and RTV.

All endpoints (including SVC-enabled endpoints) have AVC capabilities and can connect to AVC conferences running on the MCU. AVC-based endpoints can connect using different signaling protocols and different video protocols.

Based on the video processing required during the conference, the Collaboration Server offers the Continuous Presence Conferencing Mode for AVC-based conferencing.

In the Collaboration Server (RMX) 1500/2000/4000, the MCU also offers the Video Switching conferencing Mode. Video Switching is not supported with Collaboration Server (RMX) 1800.

The Conferencing Mode determines the video display options (full screen or split screen with all participants viewed simultaneously) and the method in which the video is processed by the MCU (with or without using the MCU's video resources).

Continuous Presence (CP) Conferencing

The dynamic Continuous Presence (CP) capability of the Collaboration Server system enables viewing flexibility by offering multiple viewing options and window layouts for video conferencing. It enables several participants to be viewed simultaneously and each connected endpoint uses its highest video, audio and data capabilities up to the maximum line rate set for the conference.

AVC-based endpoints can connect to the conference using any:

- Signaling protocol: H.323, SIP, ISDN/PSTN (Collaboration Server (RMX) 1500/2000/4000) and RTV line rate, up to a maximum line rate defined for the conference
- Video Protocol: H.261, H.263, H.264 Base Profile and H.264 High Profile) and at any resolution and frame rate, provided they meet the minimum requirements set for the conference:

- Video Resolutions: from QCIF, CIF and up to 1080p60
- > Frame rates up to 60fps

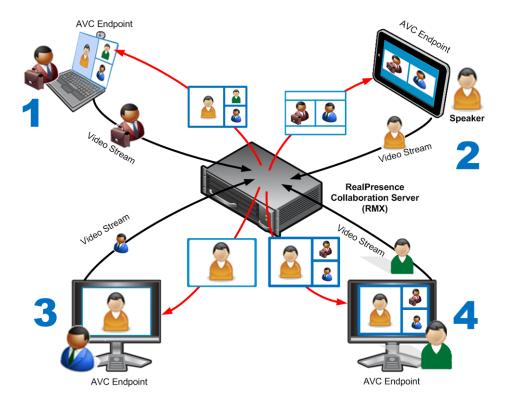
In Continuous Presence conferences, the MCU receives the video stream from each endpoint at the video rate, video resolution and frame rate that it is capable of sending, and it superimposes all the received streams into one video stream that includes the input from the other endpoints arranges in the selected video layout.

Participants do not see themselves in the video layout. By Default, the speaker is shown in the top left layout cell in symmetric layouts, in the larger cell in asymmetric layouts, or in full screen. The speaker sees the previous speakers (their number depends on the number of cells on the speaker's layout.

The Continuous Presence video session offers layouts to accommodate different numbers of participants and conference settings including support of the VUI annex to the H.264 protocol for endpoints that transmit wide video instead of 4CIF resolution. Each participant can select his/her layout for viewing during the conference, as can be seen in AVC Continuous Presence (CP) video streams and built layouts.

For conferences with more participants than display squares, the Collaboration Server dynamic video mix capability allows the viewed sites to be modified throughout the conference. The displayed layout can be changed during an ongoing conference, allowing a participant to view different screen layouts of the other conference participants. These layout options allow conferences to have greater flexibility when displaying a large number of participants and maximizes the screen's effectiveness.

AVC Continuous Presence (CP) video streams and built layouts



Video quality in Continuous Presence conferences is affected by the conference line rate (that determines the maximum line rate to be used by the connecting endpoints), and the video capabilities of the endpoints such as the video protocol, video resolution and frame rate. Content sharing is available in all CP conferences.

This requires extensive processing of the video sent to each participant in the conference. The higher the video rate and resolution, the more processing power is required.

By default every conference, Entry Queue and Meeting Room has the ability to declare the maximum CP resolution as defined for the system. This includes conferences launched by the Collaboration Server Web Client and conferences started via the API.

CP conferencing is defined in the Conference profile by setting the following main features:

- Setting the Conferencing Mode to CP only
- Conference Line Rate
- Video Quality Motion or Sharpness
- Video Layout

Video Protocol Support in CP Conferences

The video protocol selected by the system determines the video compression standard used by the endpoints. In Continuous Presence conferences, the system selects the best video protocol for each of the endpoint according to he endpoint's capabilities.

The following Video protocols are supported in CP conferences:

- **H.261** The legacy video compression algorithm mandatory to all endpoints. It is used by endpoints that do not support other protocols.
- H.263 A video compression algorithm that provides a better video quality than H.261. This standard
 is not supported by all endpoints.
- H.264 Base Profile A video compression standard that offers improved video quality, especially at line rates lower than 384 Kbps.
 - **H.264 High Profile** allows higher quality video to be transmitted at lower line rates.
- RTV A video protocol that provides high quality video conferencing capability to Microsoft OCS (Office Communicator Server) endpoints at resolutions up to HD720p30. (SIP only).

Video Switching (VSW) Conferencing

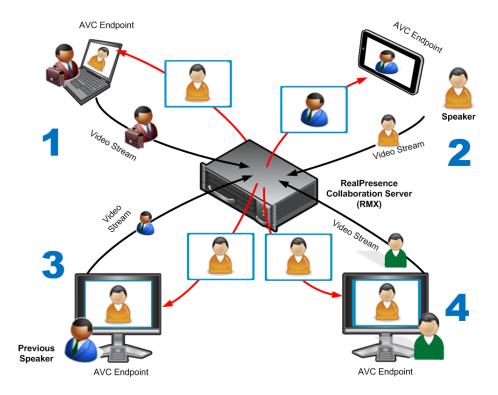


Video Switching (VSW) Conferencing is not supported with RealPresence Collaboration Server 1800.

In Video Switching mode all participants see the same video picture (full screen). The current speaker is displayed in full screen on all the participants' endpoints, while the speaker sees the previous speaker. Switching between participants is voice-activated; whenever a participant starts to speak, he or she becomes the conference speaker and is viewed on all screens. All conference participants must use the

same line rate and video parameters such as video protocol, frame rate, annexes and interlaced video mode as no video processing is performed. Endpoints that are unable to meet these requirements connect as Secondary (audio only).

AVC Video Switching (VSW) video streams and Full Screen Layout



Video Switching (VSW) Conferencing Guidelines

You can run VSW conferences when following the guidelines listed below.

- Only H.264 Base and High Profile video protocols are supported in Video Switching Conferences.
- Video Switching conferences can be set to one of the following resolutions, depending on the capabilities of the endpoints connecting to the conference:
 - ➤ H.264 1080p60 (Symmetrically, at bit rates of up to 6Mbps).
 - ➤ HD1080p60
 - > H.264 1080p30
 - ➤ H.264 720p30
 - ➤ H.264 720p60
 - > H.264 SD 30
 - > H.264 CIF (from version 7.6)
 - > H.263 CIF (from version 7.6)
 - > H.261 CIF (from version 7.6)
- Video Switching conferencing mode is unavailable to ISDN participants.

 Video Switching uses fewer system resources than CP: only one CIF video resource per participant for any resolution (including HD). The table below lists the resources available to VSW conferences by line rate and card type.

VSW Resource Capacity Line Rate

	Maximum Possible Resources Per Card*	
Resource Type	МРМх	MPMRx
VSW 2Mbps	80*	200
VSW 4Mbps	40*	100
VSW 6Mbps	20*	50

^{*} Capacity numbers are for maximum capacity card assemblies. These numbers may be lower when LPR and/or encryption are enabled.

The following table lists the recommended number of connections at *HD1080p* resolution for fully configured and licenced RealPresence Collaboration Server (RMX) systems with MPMx cards. For detailed resource capacity information see the relevant *Collaboration Server Hardware Guide*.

Maximum Number of HD1080p Connections by Line Rate

	RMX 1500	RM	IX 2000	Ri	MX 4000
Line Rate/Participants	(MPMx)	MPMx	MPMRx	MPMx	MPMRx
Up to 2Mbps	80	160	400**	320	
4Mbps	40	80		160	
6Mbps	20	40		80	

- The maximum supported video conference size is 180 participants with the MPMx card.
- The display aspect ratio is 4x3 or 16x9.
- Site (endpoint) names, skins, message overlay etc. are not supported in Video Switching.
- Video forcing is enabled at the conference and participant levels.
- To connect to a Video Switching conference via Entry Queue, the Profile assigned to the Entry Queue
 must be set to Video Switching. It is recommended to use the same profile for both the destination
 conference and Entry Queue.
- Telepresence Mode is unavailable in Video Switching conferences.
- In Collaboration Server (RMX) 2000/4000 with MPMRx media cards, each participant connecting to a VSW conference consumes one HD720 port.

The HD_THRESHOLD_BITRATE flag must be set in the System Configuration. The value of this flag
is the system minimum threshold bit rate for HD resolutions. The line rate selected in the conference
Profile must be the same as or higher than that specified by the HD_THRESHOLD_BITRATE flag.



The HD_THRESHOLD_BIT RATE flag is responsible for negotiation only, It does not guarantee that the endpoint will open an HD channel or transmit on an opened HD channel.

The **HD_THRESHOLD_BITRATE** flag line rate value ranges from 384kbps to 4Mbs, default is 768kbps. For more information, see Modifying System Flags.

AVC Basic Conferencing Parameters

The main parameters that define the quality of an AVC-based video conference and its display are:

- Line (Bit) Rate The transfer rate of video and audio streams. The higher the line (bit) rate, the better the video quality. The MCU supports the following line rates:
 - ➤ CP Conferences: 64kbps to 4096kbps (RealPresence Collaboration Server 1500/2000/4000) (RealPresence Collaboration Server 1800 supports up to 6144kpbs)
 - VSW Conferences: 64kbps to 6144kbps (RealPresence Collaboration Server 1500/2000/4000 only)
- Audio Algorithm The audio compression algorithm determines the quality of the conference audio.
- Video protocol, video format, frame rate, annexes, and interlaced video mode These
 parameters define the quality of the video images. The Collaboration Server will send video at the
 best possible resolution supported by endpoints regardless of the resolution received from the
 endpoints.
 - When Sharpness is selected as the Video Quality setting in the Conference Profile, the Collaboration Server will send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30fps.
 - ➤ H.264 High Profile protocol provides better compression of video images in line rates lower than 384 Kbps and it will be automatically selected for the endpoint if it supports H.264 High Profile. If the endpoint does not support H.264 High Profile, the Collaboration Server will try H.264 Base Profile which provides good compression of video images in line rates lower than 384 Kbps (better than H.263 and not as good as H.264 High Profile).
 - ➤ When working with Collaboration Servers at low bit rates (128, 256, or 384Kbps), HDX endpoints will transmit SD15 resolution instead of 2CIF resolution.

When using a full screen (1x1) conference layout, the Collaboration Server transmits the same resolution it receives from the endpoint.

Video resolution:

- ➤ H.261 CIF/QCIF Supported in Continuous Presence (CP) conferences at resolutions of 288 x 352 pixels (CIF) and 144 x 176 pixels (QCIF). Both resolutions are supported at frame rates of up to 30 frames per second.
- ➤ H.263 4CIF A high video resolution available to H.263 endpoints that do not support H.264. It is only supported for conferences in which the video quality is set to sharpness and for lines rates of 384kbps to 1920kbps.
- ➤ Standard Definition (SD) A high quality video protocol which uses the H.264 and H.264 High Profile video algorithms. It enables compliant endpoints to connect to Continuous Presence conferences at resolutions of 720 x 576 pixels for PAL systems and 720 x 480 pixels for NTSC systems.

- ➤ **High Definition (HD)** HD is an ultra-high quality video resolution that uses the H.264 and H.264 High Profile video algorithms. Depending on the Collaboration Server's type, compliant endpoints are able to connect to conferences at the following resolutions:
 - ♦ 720p (1280 x 720 pixels) all Collaboration Server types
 - ◆ 1080p (1920 x 1080 pixels) in Collaboration Server (RMX) 1500/1800/2000/4000
- Lost Packet Recovery (LPR) LPR creates additional packets that contain recovery information
 used to reconstruct packets that are lost during transmission.

Supplemental Conferencing Features

In addition to *basic parameters* that determine the quality of the video, additional features can be enabled, adding capabilities to the conference, or enabling special conferencing modes:

 Content Sharing (H.239) – Allows compliant endpoints to transmit and receive two simultaneous streams of conference data to enable Content sharing. H.239 is also supported in cascading conferences. Both H.263 and H.264 Content sharing protocols are supported. If all endpoints connected to the conference have H.264 capability, Content is shared using H.264, otherwise Content is shared using H.263.

For more information, see Sharing Content During Conferences.

- Video Clarity (CP Conferences only) Video Clarity applies video enhancing algorithms to incoming video streams of resolutions up to and including SD.
- Encryption Used to enhance media security at conference and participant levels.
 For more information, see Implementing Media Encryption for Secured Conferencing.
- Conference Recording The Collaboration Server enables audio and video recording of conferences using Polycom RSS recording system.
- Lecture Mode (CP Conferences only) The lecturer is seen by all participants in full screen while
 the lecturer views all conference participants in the selected video layout.

For more information, see Lecture Mode (AVC CP Only).

- Presentation Mode (CP Conferences only) When the current speaker's speech exceeds a
 predefined time (30 seconds), the conference layout automatically changes to full screen, displaying
 the current speaker as the conference lecturer on all the participants' endpoints. During this time the
 speaker's endpoint displays the previous conference layout. When another participant starts talking,
 the Presentation Mode is cancelled and the conference returns to its predefined video layout.
 Presentation mode is available with Auto Layout and Same Layout.
 - If the speaker in a video conference is an Audio Only participant, the Presentation Mode is disabled for that participant.
 - Video forcing works in the same way as in Lecture Mode when Presentation Mode is activated, that is, forcing is only enabled at the conference level, and it only applies to the video layout viewed by the lecturer.
- **Telepresence Mode (CP Conferences only)** enables the connection of numerous high definition telepresence rooms and of different models (such as TPX and RPX) into one conference maintaining the telepresence experience. This mode is enabled by a special license.
- **TIP Support (CP Conferences only)** *TIP* is a proprietary protocol created by Cisco for deployment in Cisco TelePresence systems (CTS). Polycom's solution is to allow the Collaboration Server to natively inter-operate with Cisco TelePresence Systems, ensuring optimum quality multi-screen, multipoint calls.

SVC-based Conferencing

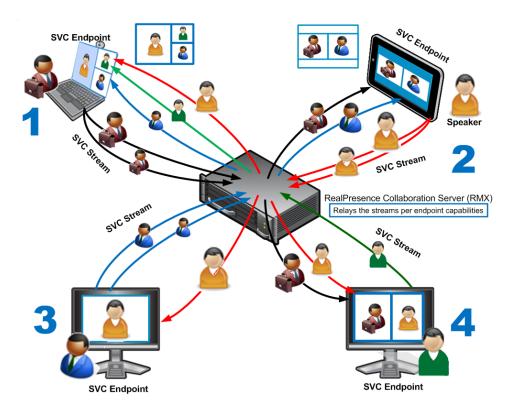
The SVC-Based conferencing mode provides video without transcoding by the MCU, hence requiring less video resources while providing better error resiliency and lower latency.

Using the SVC video protocol, SVC conferences provide video bit streams at different resolutions, frame rates and line rates to SVC-enabled endpoints with various display capabilities and layout configurations.

In the SVC-based conference, each SVC-enabled endpoint transmits multiple bit streams, called simulcasting, to the Polycom® RealPresence® Collaboration Server. Simulcasting enables each endpoint to transmit at different resolutions and frame rates such as 720p at 30fps, 15fps, and 7.5fps, 360p at 15fps and 7.5fps, and 180p at 7.5fps.

The Polycom SVC-enabled endpoints (such as Polycom® RealPresence® Desktop and Polycom® RealPresence® Mobile) compose the layout according to their layout settings and video capabilities. This enables the MCU to send or relay the selected video streams to each endpoint without processing the video streams and sending the composite video layout to the endpoints.

SVC video streams and Layouts



The video streams displayed in the conference layout on each endpoint is obtained from the different streams received from each of the endpoints displayed in the layout. Depending on the size of the video cell in the configured layout, the endpoint requests the video stream in the required resolution from the RealPresence Collaboration Server. The higher the display quality and size, the higher the requested resolution will be sent to the endpoint. The endpoint creates the displayed layout from the different video streams it receives.

For instance, an SVC endpoint might want to receive three video streams at different frame rates and resolutions, and create a conference layout with the received video streams. Each SVC-enabled endpoint sends encoded SVC bit streams to the MCU to relay to the other SVC-enabled endpoints in the conference.

The endpoints encode the video in multiple resolutions and decodes the multiple video input streams.

For example:

RealPresence mobile client (2) will transmit two resolutions; one that is suited for RealPresence Desktop client (3) and a second that is suited for two other endpoints: RealPresence Desktop client (4) and (1).

RealPresence Desktop client (1) transmits two resolutions; one that is suited for RealPresence Mobile client (2) and a second that is suited for RealPresence Desktop client (4).

The MCU determines which of the incoming resolutions to send to each endpoint. It does not perform any SVC encoding and decoding, or any transcoding of the video streams. The RealPresence Collaboration Server functions as the multipoint media relay to the endpoints. For voice activated selection of the video streams, the RealPresence Collaboration Server determines which of the incoming bit streams to send to each endpoint.

Advantages of SVC Conferencing

SVC increases the scalability of video networks and enables mass desktop video deployments. Some of the advantages of SVC conferencing are:

- Offers high-resolution video conferencing with low end-to-end latency, improved error resiliency and higher system capacities.
- Allows the SVC-enabled video endpoints to manage display layouts, supporting multiple line rates, resolutions and frame rates.
- The RealPresence Collaboration Server functions as a media relay server providing low cost production benefits. The RealPresence Collaboration Server reduces bandwidth usage by only selecting the necessary video stream to be sent to the endpoints.

SVC Conferencing Guidelines

You can run SVC-based conferences when following the guidelines listed below.

- SVC conferences are supported only with the following:
 - ➤ Collaboration Server (RMX) 2000/4000 systems with MPMx or MPMRX cards
 - Collaboration Server (RMX) 1500
 - > Collaboration Server (RMX) 1800
 - SVC Licensing
 - SIP over UDP signaling
 - SIP over TLS Signaling
 - Polycom SVC-enabled endpoints (Polycom® RealPresence® Desktop, Polycom® RealPresence® Mobile)
 - ➤ Ad Hoc conferencing via Meeting Rooms and ongoing conferences
- SVC Only conferences can run on the same MCU as AVC Only conferences.
- On Collaboration Server (RMX) 2000/4000, all the endpoints participating in a single SVC Only
 conference must be connected to the same media card and cannot be handled by different media
 cards as the SVC media streams cannot be shared between them.

- End-to-end latency on a local network (same site), is around 200msec to ensure AV sync (also known as Lip-sync).
- Dial-out is not available in SVC Only conference.
- Dial-in is available as follows:
 - AVC endpoints (participants) can only connect to an AVC conference or Mixed CP and SVC conference. When dialing into SVC Only conferences they will be disconnected and the calls fail.
 - SVC endpoints support both AVC and SVC video protocols:
 - When dialing into SVC Only conferences, they connect as SVC endpoints.
 - When dialing into AVC Only conferences, they connect as AVC endpoints. They cannot connect to an AVC conference using the SVC capabilities.
- SVC endpoints can connect to conferences via Entry Queues, however:
 - > The Entry Queue and Conference Modes must match both SVC Only or both Mixed.
 - Both the Entry Queue and the Conference must have the same line rate.
- SVC endpoints cannot be moved between conferences.
- Content is supported in H.264 (AVC).
 - > Only the **H.264 Cascade and SVC Optimized** option is supported.
 - LPR and DBA are not supported for SVC content sharing.
- In SVC Only conferences and Mixed CP and SVC conferences, Auto Layout is the default and the layout display for SVC endpoints is controlled from the endpoint application.
- Site names display on SVC endpoints is controlled from the SVC endpoints.
- When a RealPresence DMA system is part of the solution, the DMA is used as the SIP proxy and the SVC endpoint subscribes to the RealPresence DMA system for call control. If a RealPresence DMA system is not part of the solution, the SVC endpoint dial directly to the Collaboration Server using IP addresses is the SIP dialing strings.
- When Hot backup is enabled, all the conferences are created on the Slave MCU.
- When Hot Backup is activated and the Slave MCU becomes the Master MCU:
 - All AVC endpoints will be reconnected to the AVC (CP and VSW) conferences. SVC endpoints connected to AVC conferences using their AVC capabilities will be reconnected to their AVC conferences.
 - SVC endpoints cannot be reconnected to their SVC Only conferences as dial-out is not supported for SVC endpoints. These endpoints will have to manually reconnect to their SVC conferences.
- Cascading between SVC Only conferences or between AVC and SVC Only conferences is not supported.
- Gateway sessions are not supported for SVC calls.
- Reservations cannot be scheduled for SVC Only conferences.
- The following functionality and features are not supported during SVC Only conferences:
 - > FECC
 - Skins. The video cells are displayed on the endpoint's default background.
 - IVR functionality
 - Conference Gathering phase
 - Password protected conferences as DTMF input for passwords cannot be processed

- > All DTMF enabled features during the conference
- Manual selection of video layout
- Chairperson functionality
- Media Encryption
- > Recording of SVC Only conferences
- > Text messaging using Message Overlay

MCU Supported Resolutions for SVC Conferencing

The MCU automatically selects the resolution and frame rate according to the conference line rate. The table below details the maximum resolution and frame rates supported by the MCU for each conference line rate. The actual video rate, resolution and frame rates displayed on each endpoints is determined by the endpoint's capabilities.

SVC Conferencing - Maximum Supported Resolutions per Simulcast Stream

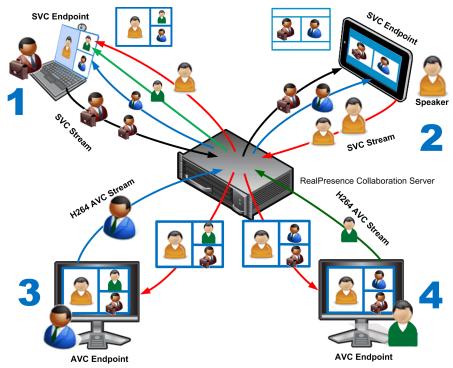
Conference Line Rate (kbps)	Profile	Maximum Resolution	Max. Frame Rate (fps)	Audio Rate (kbps)
1472 - 2048	High Profile	720p	30fps	48
1024 - 1472	High Profile	720p	15fps	48
768 - 1024	High Profile	720p	15fps	48
512 - 768	High Profile	360p	30fps	48
256 - 512	Base Profile	180p	15fps	48
192 - 256	Base Profile	180p	30fps	48
128 - 192	Base Profile	180p	15fps	48

Mixed CP and SVC Conferencing

In a mixed CP (AVC) and SVC conference, AVC-based endpoints and SVC-enabled endpoints can be supported in the same conference.

In a mixed CP (AVC) and SVC conference, SVC endpoints transmit multiple resolutions and temporal layers to the RealPresence Collaboration Server like the SVC-based conferences, while AVC endpoints, for example, send only one AVC video stream to the Collaboration Server. AVC endpoints can send different video protocoles, such as H.263, and H.264. The Collaboration Server relays SVC-encoded video bit streams to the SVC-enabled endpoints in the conference according to their request. This enables the video conference layouts to be automatically assembled by the endpoint. AVC endpoints connected to the conference send a single AVC video bit stream to the Collaboration Server, which is then transcoded to SVC video streams. SVC-enabled endpoints receive the AVC converted video bit streams through the Collaboration Server from the AVC endpoints as a single SVC video bit stream. Alternatively, AVC endpoints receive a single video bit stream with the defined video conference layout from the Collaboration Server.

The following diagram illustrates an example of a mixed CP and SVC conferencing mode:



In this example, an SVC endpoint (1) receives three video streams at different frame rates and resolutions, and creates the conference layout with the received video streams. The video bit stream that the SVC endpoint receives from the AVC endpoint (3) is decoded in the Collaboration Server and then encoded into an SVC bit stream in the required resolution.

Alternatively, an AVC endpoint (4) sends a single resolution video stream to the Collaboration Server. The Collaboration Server first decodes the SVC bit streams and AVC bit streams, then the Collaboration Server composes the video layout for the AVC endpoint and sends a single resolution video stream with the video layout to the participant. In the displayed example, the Collaboration Server creates different video layouts for each AVC endpoint.

MCU Resource Capacities for Mixed CP and SVC Conferences

In a mixed CP and SVC conference, video resources are allocated according to the MCU type and the translation pools (AVC to SVC and SVC to AVC) used to convert video streams. Translation pools are dynamically allocated, when the conference becomes a mixed CP and SVC conference; resources are not released when the conference stops being a mixed CP and SVC conference. The translation pools send one SVC to AVC stream with a resolution of 360p, two AVC to SVC streams with a resolution of 360p and 180p for AVC HD endpoints, and one video stream with a resolution of 180p for AVC SD endpoints. When a video stream with a resolution of 360p is not available, a video stream with a resolution of 180p is sent instead.

Translations between different endpoints can be done without using the highest resolution, thus saving translation resources. CP video layouts in mixed CP and SVC conferences support the standard resolutions as in normal CP conferences.

Taking these factors into consideration and the type of MCU deployed in the environment, the resource capacities for a mixed CP and SVC conference can vary.

The following table describes an example of the resource capacity allocations for the RealPresence Collaboration Server:



System Resources are now reported in terms of HD720p30 CP ports. One HD video port equals 3 CIF video ports.

Resource Capacity Allocations

	Number of Available Ports	
Resource Type	RMX 2000 2x MPMx	RMX 4000 4x MPMx
Mixed CP and SVC (HD) (Example)	20 AVC 90 SVC	40 AVC 180 SVC
HD720p30	60	120
SD (@ 30 fps)	120	240
SVC Only	180	360
CIF (@ 30 fps)	180	360

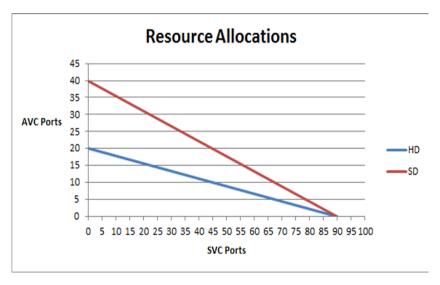
The first four resource types in the resource capacity allocations table are endpoints in a CP only conference or a mixed CP and SVC conference before the actual resource allocations occur.

In a mixed CP and SVC conference, video resources are used according to the amount of both AVC and SVC participants in the conference and according to the actual type of the conference - mixed CP and SVC conferences or CP only conferences. The ratio of resources in a mixed conference is one AVC HD (720p30) video resource to three SVC video resources, meaning for each AVC HD video resource, three SVC video resources can be allocated.

In this resource capacity allocations example, the mixed CP and SVC conference can allocate a combination of AVC and SVC ports depending on the endpoints that are defined in the actual conference. For example, a conference can be defined as a mixed CP and SVC conference but will only allocate resources as a mixed conference when both AVC and SVC endpoints join the conference. When there are only one resource type of endpoints participating in the conference, such as AVC or SVC, the resource allocations are assigned according to the type of endpoint with the system flag

MIX_AVC_SVC_DYNAMIC_ALLOCATION set to **TRUE**. For instance, a mixed CP and SVC conference with HD endpoints assigned, can have 60 or 120 ports allocated depending on the server configuration. When an SVC endpoint joins the conference, the conference becomes an actual mixed conference and the resource allocations are divided between the AVC and SVC endpoints. The Resource Report will reflect this by showing an increase in the resource usage.

The following diagram illustrates the amount of AVC to SVC port resources that are used in an actual mixed CP and SVC conference:



Using Conference Profiles

Conference Profiles include conference parameters such as Conferencing Mode, conference line rate, video and content sharing resolutions and settings, video layout, encryption, Lost Packet Recovery (LPR), etc. Profiles eliminate the need to define these parameters for each new conference created on the MCU. They are stored on the Collaboration Server and they enable you to define all types of conferences.

The maximum number of Conference Profiles that can be defined is 80.

Conference Profiles are assigned to Conferences, Meeting Rooms, Reservations and Entry Queues. The same Profile can be assigned to different conferencing entities. When modifying the Profile parameters, the changes will be Real Presence Collaboration Server (RMX) 1500/1800/2000/4000 Administrator's Guide applied to all the conferencing entities to which the profile is assigned.

Conference Profile options differ according to the selected *Conferencing Mode*. Profiles can be defined for AVC (Advanced Video Codec) CP and VSW (Collaboration Server 1500/2000/4000) conferencing Modes, SVC (Scalable Video Codec) conferencing Mode or Mixed CP and SVC Conferencing Mode.

Conference Profiles can be saved to *Conference Templates* along with all participant parameters, including their Personal Layout and Video Forcing settings. It enables administrators and operators to create, save, schedule and activate identical conferences quickly and easily.

Conferencing Parameters Defined in a Profile

When defining a new video Profile, you select the parameters that determine the video display on the participant's endpoint and the quality of the video, according to the selected Conferencing Mode. When defining a new conference Profile, the system uses default values for the selected conferencing Mode.

Conferencing Capabilities in the Various Conferencing Modes

The following table summarizes the conferencing capabilities and options available in the different Conferencing Modes.

Conferencing Capabilities in the Different Conferencing Modes

Feature	CP Only	Mixed CP & SVC	SVC Only
Conference Type			
Reservations	✓	✓	✓
Operator Conferences	✓	×	×
Entry Queues	√ ∗	√ *	√ ∗
Permanent Conference	✓	✓	✓
Cascading	√ **	√ **	*
Conferencing Feature			
IVR	✓	✓	✓
			Reduced IVR set for SVC endpoints
Dial Out	✓	*	*
Auto Redial	✓	✓	×
LPR	✓	√ ***	√ ***
Content	✓	√ ‡	✓
	All Content Settings, All Content Protocols	Graphics Only, H.264 Cascade & SVC Optimized (only)	Graphics Only, H.264 Cascade & SVC Optimized
Presentation Mode	✓	×	×
Lecture Mode	✓	*	*
Same Layout	✓	✓	×
Layout Selection	✓	✓	Layout set to Auto Layout
		AVC endpoints only	and defined on the endpoint
Skins	✓	✓	×
		AVC endpoints only	
Encryption	√	✓	✓

Conferencing Capabilities in the Different Conferencing Modes

Feature	CP Only	Mixed CP & SVC	SVC Only	
Recording	✓	✓	×	
		AVC recording only		
Site Names	✓	✓	Managed by the endpoint (not via MCU)	
		AVC endpoints only		
Message Overlay	✓	✓	×	
		AVC endpoints only		

^{*} Entry Queue & Destination Conference must have the same profile (i.e. SVC only to SVC only, Mixed CP and SVC to Mixed CP and SVC)

Default Profile Settings in CP Conferencing Mode

The Collaboration Server is shipped with a default Conference Profile for CP conferences which allows users to immediately start standard ongoing CP conferences. These are also the default settings when creating a new Profile. The default settings are as follows:

Default CP Only Conference Profile Settings

Setting	Value
Profile Name	Factory_Video_Profile
Line Rate	384Kbps
Video Switching	Disabled
Operator Conference	Disabled
Encryption	Disabled
Packet Loss Compensation (LPR and DBA)	Enabled for CP Conferences
Auto Terminate	After last participant quits - EnabledWhen last participant remains - Disabled
Auto Redialing	Disabled
Exclusive Content Mode	Disabled
TIP Compatibility	Disabled
Enable FECC	Enabled
Enabled Gathering Phase	Enabled

^{**} Only Basic Cascading is available

^{***} For AVC, the LPR error resiliency is used, however for SVC endpoints, new error resiliency methods are used.

^{‡.} Content Line Rate is fixed at 128Kbps.

Default CP Only Conference Profile Settings

Setting	Value
Display Language	English
Video Quality	Sharpness
Maximum Resolution	Auto
Video Clarity	Enabled
Auto Brightness	Enabled
Content Settings	HiResGraphics (High Res Graphics)
Content Protocol	H.264 HD
Send Content to legacy endpoints	Enabled
Presentation Mode	Disabled
Same Layout	Disabled
Lecturer View Switching	Disabled
Telepresence Mode	Auto
Telepresence Layout Mode	Continuous Presence
Auto Scan Interval	Disabled (10)
Auto Layout	Enabled
Echo Suppression	Enabled
Keyboard Noise Suppression	Disabled
Audio Clarity	Enabled
Mute participants except the lecturer	Disabled
Skin	Polycom
IVR Name	Conference IVR Service
Recording	Disabled
Site Names display	Disabled
Message Overlay	Disabled
Network Services - SIP Registration	Disabled
Network Services - Accept Calls	Enabled

This Profile is automatically assigned to the following conferencing entities:

Name	ID	
Meeting Rooms		
Maple_Room	1001	
Oak_Room	1002	
Juniper_Room	1003	
Fig_Room	1004	
Entry Queue		
Default EQ	1000	

Default Profile Settings in SVC Only Conferencing Mode

The Collaboration Server is shipped with a default Conference Profile for SVC Only conferences which allows users to immediately start standard ongoing SVC Only conferences. These are also the default settings when creating a new Profile. The default settings are as follows:

Default SVC Only Conference Profile Settings

Setting	Value
Profile Name	Factory_SVC_Video_Profile
Line Rate	1920Kbps
Video Switching	Disabled
Operator Conference	Not supported
Encryption	Disabled
Packet Loss Compensation (LPR and DBA)	Not supported
Auto Terminate	After last participant quits - EnabledWhen last participant remains - Disabled
Auto Redialing	Not supported
Exclusive Content Mode	Disabled
TIP Compatibility	Disabled
Enable FECC	Disabled
Enabled Gathering Phase	Enabled
Display Language	English
Video Quality	Sharpness

Default SVC Only Conference Profile Settings

Setting	Value
Maximum Resolution	Auto
Video Clarity	Enabled
Auto Brightness	Enabled
Content Settings	Graphics
Content Protocol	H.264 Cascading and SVC Optimized
Presentation Mode	Not applicable
Send Content to legacy endpoints	Disabled
Same Layout	Not applicable
Lecturer View Switching	Not applicable
Telepresence Mode	Auto
Telepresence Layout Mode	Continuous Presence
Auto Scan Interval	Not applicable
Auto Layout	Enabled (Only available option)
Echo Suppression	Enabled
Keyboard Noise Suppression	Disabled
Audio Clarity	Enabled
Mute participants except the lecturer	Not applicable
IVR Name	Conference IVR Service
Message Overlay	Disabled
Network Services - SIP Registration	Disabled
Network Services - Accept Calls	Enabled

Default Profile Settings in a Mixed CP and SVC Conferencing Mode

The Collaboration Server is shipped with a default Conference Profile (CP and SVC) for mixed CP and SVC conferences which enables users to immediately start a standard ongoing mixed CP and SVC conference. These are also the default settings when creating a new Profile. (During mixed SVC & CP conferences, PSTN (Audio Only) calls are supported.) Dial-out is not available in Mixed CP and SVC conferences.

The default settings are as follows:

Default Mixed CP and SVC Conference Profile Settings

Setting	Value
Profile Name	Factory_Mix_SVC_CP_Video_Profile
Line Rate	1920Kbps
Video Switching	Disabled
Operator Conference	Disabled
Encryption	Enabled
Packet Loss Compensation (LPR and DBA)	Enabled for AVC participants only
Auto Terminate	After last participant quits - EnabledWhen last participant remains - Disabled
Auto Redialing	Disabled
Font for text over video	Enabled for AVC participants only
Exclusive Content Mode	Disabled
TIP Compatibility	Disabled
Enable FECC	Enabled
Enabled Gathering Phase	Enabled
Display Language	English
Video Quality	Sharpness
Maximum Resolution	Auto
Video Clarity	Disabled
Auto Brightness	Disabled
Content Settings	Graphics
Content Protocol	H.264 Cascade and SVC Optimized (only)
Presentation Mode	Disabled
Send Content to legacy endpoints	Disabled
Same Layout	Enabled
Lecturer View Switching	Disabled
Telepresence Mode	Off
Telepresence Layout Mode	Continuous Presence
Auto Scan Interval	Disabled

Default Mixed CP and SVC Conference Profile Settings

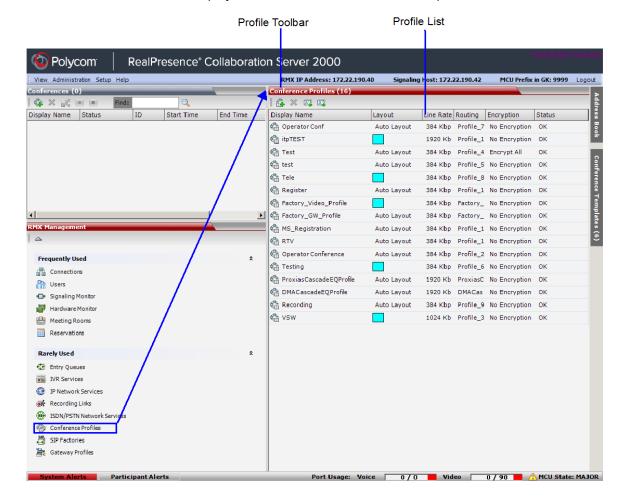
Setting	Value
Auto Layout	Enabled
Echo Suppression	Enabled for AVC participants only
Keyboard Noise Suppression	Enabled for AVC participants only
Audio Clarity	Enabled for AVC participants only
Mute participants except the lecturer	Disabled
Skin	Classic (for AVC participants)
IVR Name	Conference IVR Service
Recording	Enabled
Site Names display	Enabled for AVC participants only
Message Overlay	Disabled
Network Services - SIP Registration	Disabled
Network Services - Accept Calls	Enabled
Network quality indication	Enabled for AVC participants only

Viewing the List of Conference Profiles

Existing Conference Profiles are listed in the Conference Profiles list pane.

To list Conference Profiles:

- 1 In the RMX Management pane, expand the Rarely Used list.
- 2 In the RMX Management pane, Click the Conference Profiles button.



The Conference Profiles are displayed in the Conference Profiles list pane.

The number of the currently defined Conference Profiles appears in the title of the list pane. The following Conference Profile properties are displayed in the List pane:

Conference Profiles Pane Columns

Field	Description	
Name	The name of the Conference Profile.	
Layout	Displays either Auto Layout or an icon of the layout selected for the profile.	
Line Rate	The maximum bit rate in kbps at which endpoints can connect to the conference.	
Routing Name	Displays the Routing Name defined by the user or automatically generated by the system.	
Encryption	Displays if media encryption is enabled for the Profile. For more information see Packet Loss Compensation (LPR and DBA) AVC CP Conferences .	

Profiles Toolbar

The Profile toolbar provides quick access to the Profile functions:

Profile Toolbar buttons

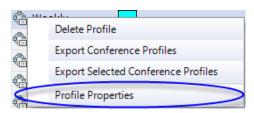
Button	Button Name	Description
	New Profile	To create a new Profile.
*	Delete Profile	To delete a Profile, click the Profile name and then click this button.
P	Import Profile	To import Conference Profiles from another MCU in your environment.
8	Export Profile	To export Conference Profiles to a single XML file that can be used to import the Conference Profiles on multiple MCUs.

Modifying an Existing Profile

You can modify any of the Profile's parameters but you cannot rename the Profile.

To modify the Profile properties:

1 In the Conference Profiles List, double-click the Profile icon or right-click the Profile icon, and select Profile Properties.



The Profile Properties - General dialog box opens.

- 2 Modify the required Profile parameter(s).
- 3 Click OK.

Deleting a Conference Profile

You can delete Profiles from the Profiles list.



A Conference Profile cannot be deleted if it is being used by Meeting Rooms, Reservations, Entry Queues, and SIP Factories. A Profile that is assigned to only one ongoing conference and no other conferencing entity can be deleted.

To delete a Conference Profile:

- 1 List the Profile that are currently defined in the system. For details, see Viewing the List of Conference Profiles.
- 2 In the Conference Profiles list, select the Conference Profile you want to delete.
- 3 Click the **Delete Profile** (X) button.

or

Right-click the Conference Profile you wish to delete, and select Delete Profile from the menu.

4 In the confirmation dialog box, click **OK**.

The Conference Profile is deleted.

Defining New Profiles

Profiles are the basis for the definition of all ongoing conferences, Reservations, Meeting Rooms, Entry Queues, and Conference Templates and they contain only conference properties.

Profiles can be defined for the following **Conferencing Modes**: AVC (Advanced Video Codec) CP and VSW, SVC (Scalable Video Codec) or Mixed CP and SVC. The Profile tabs and options change according to the selected Conferencing Mode and only supported options are available for selection. Unsupported options are disabled (grayed out).

CP Conferencing Mode also offers a special functional conference - Operator Conference.

To facilitate the definition process of a new Profile, the system displays default values for each parameter so you need only to modify the required settings.

To define a new Profile:

- 1 In the RMX Management pane, expand the Rarely Used list.
- 2 In the RMX Management pane, click Conference Profiles.
- 3 In the Conference Profiles pane, click the New Profile button.
 - The New Profile General dialog box opens.
- 4 In the **Display Name** field, enter the Profile name.
- 5 Select the appropriate Conferencing Mode: CP, VSW (Collaboration Server 1500/2000/4000), SVC Only or CP and SVC.

The New Profile tabs and options change according to the selected Conferencing Mode and only supported options are available for selection.

- 6 Define the Profile parameters as described in:
 - Defining AVC CP Conferencing Profiles
 - Defining an AVC Video Switching Conference Profile
 - Defining SVC Conference Profiles
 - Defining Mixed CP and SVC Conferencing Profiles

Exporting and Importing Conference Profiles

Conference Profiles can be exported from one MCU and imported to multiple MCUs in your environment, enabling you to copy the Conference Profiles definitions to other systems. This can save configuration time and ensures that identical settings are used for conferences running on different MCUs. This is especially important in environments using cascading conferences that are running on different MCUs.

Guidelines for Exporting and Importing Conference Profiles

- Only Collaboration Server system administrators can export and import Conference Profiles.
 Operators are only allowed to export Conference Profiles.
- You can select a single, multiple, or all Conference Profiles to be exported.
- Conference Templates and their related Conference Profiles can be exported and imported simultaneously using the Conference Templates export and import function. For more information, see Exporting and Importing Conference Templates.

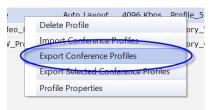
Exporting Conference Profiles

Conference Profiles are exported to a single XML file that can be used to import the Conference Profiles on multiple MCUs. Using the Export Conference Profile feature, you can export all or selected Conference Profiles from an MCU.

Exporting All Conference Profiles from an MCU

To export all Conference Profiles from an MCU:

- 1 List the Profile that are currently defined in the system. For details, see Viewing the List of Conference Profiles.
- 2 In the Conference Profiles List toolbar, click the **Export Conference Profiles** button or right-click anywhere in the Conference Profiles pane, and then click **Export Conference Profiles**.

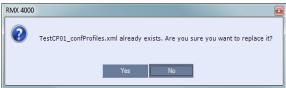


The Conference Profile - Export dialog box is displayed.



- 3 In the **Export Path** field, click **Browse** to navigate to the location of the desired path where you want to save the exported file.
- 4 In the Profiles file name field, type the file name prefix. The file name suffix (_confProfiles.xml) is predefined by the system. For example, if you type Profiles01, the exported file name is defined as Profiles01 confProfiles.xml.
- 5 Click **OK** to export the Conference Profiles to a file.

If the export file with the same file name already exists, a prompt is displayed.



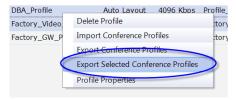
6 Click **Yes** to replace the exported file, or click **No** to cancel the export operation and return to the Conference Profiles list. You can modify the export file name and restart the export operation.

Exporting Selected Conference Profiles

You can select a single Conference Profile or multiple Conference Profiles and export them to a file to be imported to other MCUs in your environment.

To export selected Conference Profiles:

- 1 List the Profile that are currently defined in the system. For details, see Viewing the List of Conference Profiles.
- 2 In the Conference Profiles pane, select the profiles you want to export.
- In the Conference Profiles List toolbar, click the Export Conference Profiles button or right-click the selected Conference Profiles, and then click Export Selected Conference Profiles.

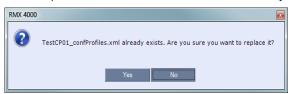


The Conference Profile - Export dialog box is displayed.



- 4 In the **Export Path** field, click **Browse** to navigate to the location of the desired path where you want to save the exported file.
- 5 In the Profiles file name field, type the file name prefix. The file name suffix (_confProfiles.xml) is predefined by the system. For example, if you type Profiles01, the exported file name is defined as Profiles01 confProfiles.xml.
- 6 Click **OK** to export the Conference Profiles to a file.

If the export file with the same file name already exists, a prompt is displayed.



7 Click Yes to replace the exported file or click No to cancel the export operation and return to the Conference Profiles list. You can modify the export file name and restart the export operation.

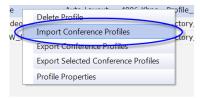
Importing Conference Profiles

If your environment includes two or more MCUs, import previously exported Conference Profiles to your MCU to save configuration time and ensure that all MCUs use the same conferencing parameters.

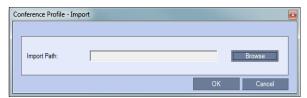
Conference Profiles are not imported when a Conference Profile with that name already exists or if an IVR Service which is assigned to any of the imported Profile does not exist in the MCU.

To import Conference Profiles:

- 1 Display the Conference Profiles List. For details, see Viewing the List of Conference Profiles .
- 2 In the Conference Profiles List toolbar, click the **Import Conference Profiles** button or right-click the Conference Profiles pane, and then click **Import Conference Profiles**.

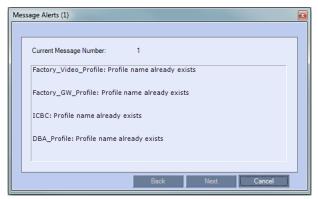


The Conference Profile - Import dialog box is displayed.



- 3 In the **Import Path** field, click **Browse** to navigate to the path and file name of the exported Conference Profiles you want to import.
- 4 Click **OK** to import the Conference Profiles.

When Conference Profiles cannot be imported, a **Message Alert** window is displayed with the profiles that were not imported.



Conference Profiles that are not problematic are imported.

5 Click Cancel to exit the Message Alerts window.

The imported Conference Profiles appear in the Conference Profiles list.

Defining AVC-Based Conference Profiles

AVC-based Conference Profile options differ according to the selected Conferencing Mode CP and VSW (Collaboration Server 1500/2000/4000 only). To facilitate the definition process of a new Profile, the system displays default values for each parameter so you need only to modify the required settings.



The following features are not supported with Collaboration Server 1800:

- ISDN/PSTN connections
- Video Switching Conferences
- · Gateway Calls

Any reference to these features relates to the RealPresence® Collaboration Server 1500/2000/4000.

Defining AVC CP Conferencing Profiles

When defining a new Profile, you select the parameters that determine the video display on the participant's endpoint, the quality of the video, content sharing parameters, whether the conference will be recorded, encryption, Telepresence mode and other conferencing parameters.

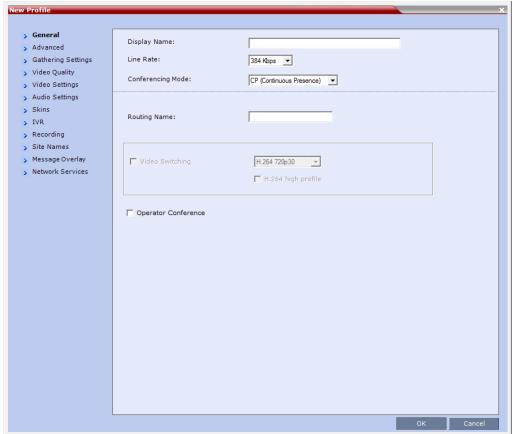
The following parameters are defined:

- New AVC CP Profile General Parameters
- New AVC CP Profile Advanced Parameters
- New AVC CP Profile Gathering Settings Parameters
- New AVC CP Profile Video Quality Parameters
- New AVC CP Profile Video Settings Parameters
- New AVC CP Profile Audio Settings Parameters
- New AVC CP Profile IVR Parameters
- New AVC CP Profile Recording Parameters
- New AVC CP Profile Site Names Parameters
- New AVC CP Profile Message Overlay Parameters
- New AVC CP Profile Network Services Parameters

To define a new CP Profile:

- 1 In the RMX Management pane, click Conference Profiles.
- 2 In the Conference Profiles pane, click the New Profile button.





3 Define the Profile name and, if required, the Profile General parameters:

New AVC CP Profile - General Parameters

Field/Option	Description
Display Name	 Enter a unique Profile name, as follows: English text uses ASCII encoding and can contain the most characters (length varies according to the field). European and Latin text length is approximately half the length of the maximum. Asian text length is approximately one third of the length of the maximum. It is recommended to use a name that indicates the Profile type, such as CP or Operator conference.
	Notes:This is the only parameter that must be defined when creating a new profile.This field is displayed in all tabs.

New AVC CP Profile - General Parameters

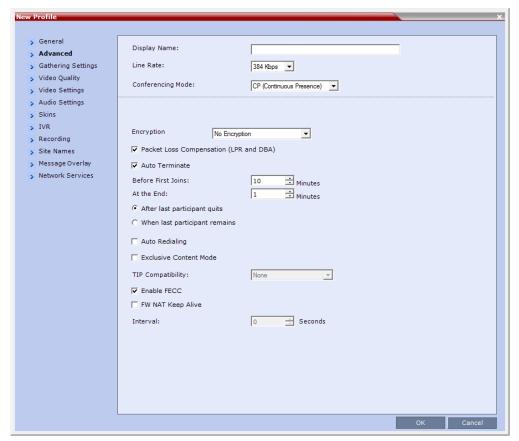
Field/Option	Description
Line Rate	Select the conference bit rate. The line rate represents the combined video, audio and Content rate.
	The default setting is 384 Kbps.
	Notes:
	 In the Collaboration Server 1500/2000/4000, the maximum line rate at which ISDN endpoints can connect to a conference is 768 kbps.
	This field is displayed in all tabs.
	 The Collaboration Server (RMX) 1800 supports AVC-CP conferences at line rates up to and including 6Mbps:
	For Dial-in calls only.
	For use with HD1080p30/60 and HD720p60 resolutions.
	To prevent excessive bandwidth usage and resource consumption, the system will ignore a Line Rate of 6Mbps, substituting line rates appropriate to the Maximum Resolution defined.
Conferencing Mode	Select the required Conferencing Mode. The selection affects the available tabs and their fields.
	For CP conferencing, make sure that CP (Continuous Presence) is selected to define a CP conference Profile (it is the default option).
	Notes:
	This field is displayed in all tabs.
	 If, while a Line Rate of 6Mbps is selected, the Conferencing Mode is changed from AVC-CP to SVC Only or CP and SVC conferencing mode, the line rate should also be changed to 1920Kbps, which is the default line rate for this conferencing mode.
	If a the selected conference Line Rate and Conferencing Mode are not compatible an error message is displayed.
	RMX The selected Conference Line Rate is too low to support the selected Content Line Rate. Click Cancel and reconfigure either of the Line Rates or click OK to return to the default Content Setting.
	OK Cancel
Routing Name	Enter the Profile name using ASCII characters set.
	The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows:
	 If an all ASCII text is entered in Display Name, it is used also as the Routing Name.
	 If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.
Video Switching	This option is disabled when CP is selected as the Conferencing Mode. For more information, see Defining an AVC Video Switching Conference Profile.
H.264 High Profile	Select this check box to enable the use of H.264 High Profile in Video Switching conferences. For more information, see H.264 High Profile Support in Video Switching Conferences.

New AVC CP Profile - General Parameters

Field/Option	Description
Operator Conference (CP Only)	Select this option to define the profile of an Operator conference. An Operator conference can only be a Continuous Presence conference, therefore when selected, the Video Switching option is disabled and cleared (Collaboration Server 1500/2000/4000). When defining an Operator Conference, the Send Content to Legacy Endpoints option in the Video Quality tab is cleared and disabled. For more information, see Operator Assistance & Participant Move.

4 Click the Advanced tab.

The New Profile - Advanced dialog box opens.



5 Define the following parameters:

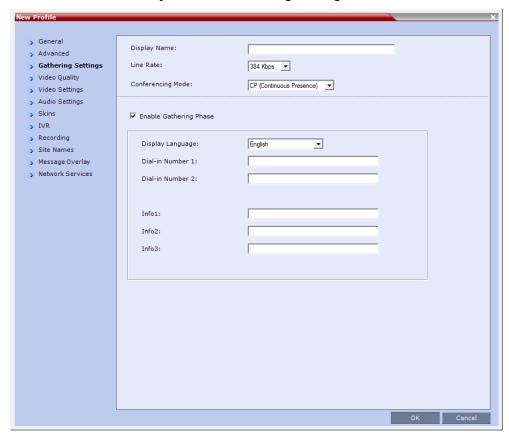
New AVC CP Profile - Advanced Parameters

Field/Option	Description
Encryption	Select the Encryption option for the conference:
	 Encrypt All - Encryption is enabled for the conference and all conference participants must be encrypted.
	 No Encryption - Encryption is disabled for the conference.
	 Encrypt when Possible - Enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. For connection guidelines see Mixing Encrypted and Non-encrypted Endpoints in one Conference.
	For more information, see Packet Loss Compensation (LPR and DBA) AVC CP Conferences.
LPR	When selected (default for CP conferences), <i>Lost Packet Recovery</i> creates additional packets that contain recovery information used to reconstruct packets that are lost during transmission.
	In Collaboration Server (RMX) 1500/2000/4000, the LPR check box is automatically cleared if Video Switching is selected as the Conferencing Mode, but can be selected if required. For more information, see Packet Loss Compensation (LPR and DBA) AVC CP Conferences.
Auto Terminate	When selected (default), the conference automatically ends when the termination conditions are met:
	• Before First Joins — No participant has connected to a conference during the <i>n</i> minutes after it started. Default idle time is 10 minutes.
	 At the End - After Last Quits — All the participants have disconnected from the conference and the conference is idle (empty) for the predefined time period. Default idle time is 1 minute.
	 At the End - When Last Participant Remains — Only one participant is still connected to the conference for the predefined time period (excluding the recording link which is not considered a participant when this option is selected). In Collaboration Server (RMX) 1500/2000/4000, this option should be selected when defining a Profile that will be used for Gateway Calls and you want to ensure that the call is automatically terminated when only one participant is connected. Default idle time is 1 minute.
	Note: The selection of this option is automatically cleared and disabled when the <i>Operator Conference</i> option is selected. The Operator conference cannot automatically end unless it is terminated by the Collaboration Server User.
Auto Redialing	The Auto Redialing option instructs the Collaboration Server to automatically redial H.323 and SIP participants that have been abnormally disconnected from the conference.
	Auto Redialing is disabled by default.
	 Auto Redialing can be enabled or disabled during an ongoing conference using the Conference Properties – Advanced dialog box.
	 The Collaboration Server will not redial an endpoint that has been disconnected from the conference by the participant.
	 The Collaboration Server will not redial an endpoint that has been disconnected or deleted from the conference by an operator or administrator.

New AVC CP Profile - Advanced Parameters

Field/Option	Description
Exclusive Content Mode	Select this option to limit the Content broadcasting to one participant, preventing other participants from interrupting the Content broadcasting while it is active.
TIP Compatibility	Select the TIP Compatibility mode when implementing an Collaboration Server and Cisco Telepresence Systems (CTS) Integration solution. The TIP Compatibility mode affects in the user video and content experience. The following TIP Compatibility modes are available: None Video Only Video & Content Prefer TIP From Version 8.1.1, Polycom endpoints can also connect to Entry Queues, Meeting Rooms and conferences using the TIP protocol. The connection of the Polycom endpoints with TIP protocol to a TIP Compatible Entry Queues, Meeting Rooms and conferences using the TIP protocol is enabled when the Polycom endpoints are registered to the CUCM and the Prefer TIP option is selected in the conference Profile. When the Prefer TIP option is selected, conferencing entities can include endpoints connected using all protocols, including TIP and SIP protocols. When Prefer TIP is selected, Gathering Settings, content settings, Message Overlay, Site Names and Network Indication(s) cannot be enabled. Note: If an option other than None is selected in this field, the Gathering Settings options are disabled. For more information, see Collaboration With Cisco's Telepresence Interoperability Protocol (TIP).
Enable FECC	This option is enabled by default, allowing participants in the conference to control the zoom and PAN of other endpoints in the conference via the FECC channel. Clear this check box to disable this option for all conference participants.
FW NAT Keep Alive	The MCU can be configured to send a FW NAT Keep Alive message at specific Intervals for the RTP, UDP and BFCP channels. For more information see FW (Firewall) NAT Keep Alive.
Interval	If needed, modify the NAT Keep Alive Interval field within the range of 1 - 86400 seconds. For more information see FW (Firewall) NAT Keep Alive.





7 Optional. Define the following fields if the conference is not launched by the Polycom Conferencing Add-in for Microsoft Outlook:



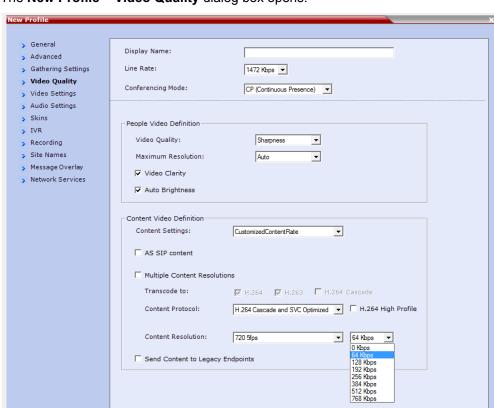
- If the conference is launched by the Polycom Conferencing Add-in for Microsoft Outlook the field information is received from the meeting invitation and existing field value are overridden. For more information see Polycom Conferencing for Microsoft Outlook®.
- In Collaboration Server 1500/2000/4000, starting with Version 7.2 the Gathering option is disabled in gateway calls.
- · Gathering is not supported in Cascading Conferences.

New AVC CP Profile - Gathering Settings Parameters

Field	Description
Display Name	This field is defined when the Profile is created. For more information see the Defining New Profiles.
Enable Gathering	Select this check box to enable the Gathering Phase feature. Default: Selected.
Displayed Language	Select the Gathering Phase slide language: Gathering Phase slide field headings are displayed in the language selected. The Gathering Phase slide can be in a different language to the Collaboration Server Web Client. Default: English Note: When working with the Polycom Conferencing Add-in for Microsoft Outlook, the language selected should match the language selected for the conference in the Polycom Conferencing Add-in for Microsoft Outlook to ensure that the Gathering
	Phase slide displays correctly.
Access Number 1	Enter the ISDN or PSTN number(s) to call to connect to the conference.
Access Number 2	Note: The numbers entered must be verified as the actual Access Numbers.
Info 1	Optionally, enter any additional information to be displayed during the Gathering Phase. These fields are not limited in the Collaboration Server Web Client but only 96 characters can be displayed in the Gathering Slide on a 16:9 monitor. If the Gathering slide is displayed on a 4:3 endpoint: the slide is cropped on both sides:
Info 2	 The left most characters of the information fields are not displayed. The live video is cropped on the right side of the display.
Info 3	Duration: 1 hour RMX 4000 go to market plan Size Brown Wide participate 5 Auto participate 5 Auto participate 6 Autopate Size Incomes Access numbers 6780123 6790123
	Info 2 Info 3 To: assistance, please call \$19 for your safety, this conference is being record

For more information see Auto Scan and Customized Polling in Video Layout (CP Conferences Only).

8 Click the Video Quality tab.



The New Profile - Video Quality dialog box opens.

9 Define the following parameters:

New AVC CP Profile - Video Quality Parameters

Field/Option	Description
People Video Defi	inition
Video Quality	Sharpness is the only supported content format that supports higher video resolutions.
	Depending on the amount of movement contained in the conference video, select either:
	 Motion – For a higher frame rate without increased resolution. When selected, Video Clarity is disabled.
	• Sharpness – For higher video resolution and requires more system resources.
	Note: When Sharpness is selected as the Video Quality setting in the conference Profile, the Collaboration Server will send 4CIF (H.263) at 15fps instead of CIF (H.264) at 30fps.

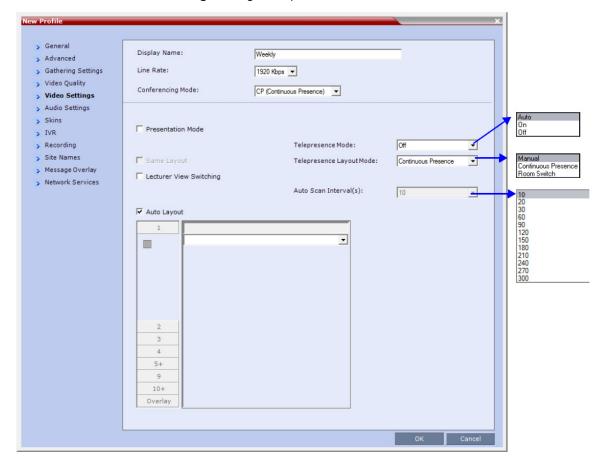
Field/Option	Description
Maximum Resolution	This setting overrides the Maximum Resolution setting of the Resolution Configuration dialog box. The administrator can select one of the following Maximum Resolution options: • Auto (default) - The Maximum Resolution remains as selected in the Resolution Configuration dialog box. • CIF • SD • HD720 • HD1080 Maximum Resolution settings can be monitored in the Profile Properties - Video Quality and Participant Properties - Advanced dialog boxes. Notes: • The Resolution field in the New Participant - Advanced dialog box allows Maximum Resolution to be further limited per participant endpoint. • The Maximum Resolution settings for conferences and participants cannot be changed during an ongoing conference.
Video Clarity™	When enabled (default), video enhancing algorithms is applied to incoming video streams of resolutions up to and including SD. Clearer images with sharper edges and higher contrast are sent back to all endpoints at the highest possible resolution supported by each endpoint. All layouts, including 1x1, are supported. Notes: Video Clarity is enabled only when Video Quality is set to Sharpness (default setting) and is disabled when Video Quality is set to Motion.
	 In Collaboration Server (RMX) 1500/2000/4000 Video Clarity can only be enabled for Continuous Presence conferences in MPMx and MPMRx Card Configuration Modes.
Auto Brightness	 Auto Brightness detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout. Auto Brightness only increases brightness and does not darken video windows. Auto Brightness is selected by default. Auto Brightness cannot be selected and deselected during an ongoing conference. When Auto Brightness is enabled, color changes may be observed in computer-based VGA Content sent by HDX endpoints through the People video channel. Default: On Note:
	 In Collaboration Server (RMX) 1500/2000/4000, Auto Brightness is supported with MPMx and MPMRx cards only.

Field/Option	Description
Content Video Defi	nition
Content Video Den	 Select the transmission mode for the Content channel: Graphics — basic mode, intended for normal graphics Hi-res Graphics (AVC CP Only) — a higher bit rate intended for high resolution graphic display Live Video (AVC CP Only) — Content channel displays live video Customized Content Rate (AVC CP Only) — manual definition of the Conference Content Rate, mainly for cascading conferences. Selection of a higher bit rate for the Content results in a lower bit rate for the people channel. For a detailed description of each of these options, see Content Sharing
AS SIP Content	Parameters in Content Highest Common (Content Video Switching) Mode. This Content Sharing option is not supported with RealPresence Collaboration Server (RMX) 1800. AS-SIP is an implementation of SIP that utilizes SIP's built in security features. When selected, content is shared using the Multiple Resolutions mode and is not supported in any other Content sharing mode. For more information, see Enabling AS-SIP Content.
Multiple Content Resolutions	Click this check box to enable the Multiple Content Resolutions mode, in which content is shared in multiple streams, one for each video protocol: H.263 and H.264. This allows endpoints with different protocols to connect and disconnect without having to restart Content sharing in the middle of a conference. For more information, see Sharing Content Using Multiple Content Resolutions Mode. When enabled, the H.264 is always selected and can not be deselected. Note: If Multiple Content Resolutions is selected in a Cascading environment, the Content Protocol must be set to H.264 Cascade and SVC Optimized and H.264 Cascade must be checked as the Transcode to: setting. Optional. Select additional protocols: H.263 - if the conference will include H.263-capable endpoints that do not support H.264 protocol for content sharing. H.264 Cascade - if the conference will include cascading links that should use a fixed video format for content sharing. Optional. If H.264 Cascade is selected, select the desired Content Resolution.

Field/Option Description Content Protocol Select the Content Protocol to be used for content sharing in Highest Common Content Sharing Mode. H.263 (AVC CP only) Content is shared using the H.263 protocol. Use this option when most of the endpoints support H.263 and some endpoints support H.264. H.263 & H.264 Auto Selection (AVC CP only) When selected, content is shared using H.263 if a mix of H.263-supporting and H.264-supporting endpoints are connected, or **H.264** if all connected endpoints have H.264 capability. H.264 Cascade and SVC Optimized All Content is shared using the H.264 content protocol and is optimized for use in cascaded conferences. H.264 HD (AVC CP only, default) Ensures high quality Content when most endpoints support H.264 and HD resolutions. Note: When Multiple Content Resolutions is selected, the Content Protocol field is hidden. For more information, see Content Protocols and Defining Content Sharing Parameters for a Conference H.264 High Profile The H.264 High Profile check box is un-checked by default and is displayed next to (Check Box) the Content Protocol drop-down menu if all the following conditions are met: The MCU is a RealPresence Collaboration Server 1800, or 2000/4000 containing MPMRx cards. The selected Conferencing Mode is AVC-CP. Multiple Resolutions (Content Transcoding) is not selected. The selected Content Protocol is H.264 HD, H.264 Cascade and SVC Optimized or H.263 and H.264 Auto Selection. If H.264 HD, H.264 Cascade and SVC Optimized is selected, the Content Resolution is set according to the line rate and the H.264 Profile (Baseline Profile or High Profile). If H.263 and H.264 Auto Selection is selected, the Content Resolution is automatically set according to the line rate and the H.264 High Profile check box is automatically unchecked and disabled. TIP Compatibility (in the Profile - Advanced dialog box) is selected as None or Video Only. Content Resolution Select the Content Resolution and frame rate according to the selected Content Sharing Mode (Highest common Content or Multiple Resolution Contents) and the video protocol. For more information, see Defining Content Sharing Parameters for a Conference.

Field/Option	Description
Content Rate drop-down menu	The Content Rate drop-down menu is displayed next to the Content Resolution drop-down menu when:
	 H.264 Cascade and SVC Optimized is the selected Content Protocol and
	CustomizedContentRate is the selected Content Setting.
	The Content Rate is dependent on the MCU type (RealPresence Collaboration Server with MPMRx or RealPresence Collaboration Server 1800) and can be up to 66% of the conference line rate. In MCUs with MPMRx cards the Content Rate is limited to 2048 kbps, while when used with the RealPresence Collaboration Server 1800 the Content Rate is limited to 4096 kbps.
Send Content to Legacy Endpoints (CP only)	When enabled (default), Content can be sent to H.323/SIP/ISDN (Collaboration Server (RMX) 1500/2000/4000) endpoints that do not support H.239 Content (legacy endpoints) over the video (people) channel. For more information see Sending Content to Legacy Endpoints (AVC Only). Notes:
	 This option is enabled in MPMx and MPMRx Card Configuration Modes only
	(Collaboration Server (RMX) 1500/2000/4000).
	When enabled, an additional HD video resource is allocated to the conference.
	 This option is valid when sending Content as a separate stream is enabled by setting the System Flag ENABLE_H239 to YES.
	Select this option when Avaya IP Softphone will be connecting to the conference.
	 In Video Switching Conferencing Mode the Send Content to Legacy Endpoints option is disabled (Collaboration Server (RMX) 1500/2000/4000).
	 If the Same Layout option is selected, the Send Content to Legacy Endpoints selection is cleared and is disabled.
	Once an endpoint is categorized as Legacy, it will not be able to restore its content to the Content channel and will receive content only in the video channel.

10 Click the Video Settings tab.



The New Profile - Video Settings dialog box opens.

11 Define the video display mode and layout using the following parameters:

New AVC CP Profile - Video Settings Parameters

Field/Option	Description
Presentation Mode (CP only)	Select this option to activate the Presentation Mode. In this mode, when the current speaker speaks for a predefined time (30 seconds), the conference changes to Lecture Mode. When another participant starts talking, the Presentation Mode is cancelled and the conference returns to the previous video layout.
Same Layout (CP only)	Select this option to force the selected layout on all participants in a conference. Displays the same video stream to all participants and personal selection of the video layout is disabled. In addition, if participants are forced to a video layout window, they can see themselves.

New AVC CP Profile - Video Settings Parameters

Field/Option	Description
Lecture View Switching	Select this option to enable automatic switching of participants on the Lecturer's screen when Lecture Mode is enabled for the conference. The automatic switching is enabled when the number of participants exceeds the number of video windows displayed on the Lecturer's screen. Note: Lecture Mode is enabled in the Conference Properties – Participants tab. For more information, see Lecture Mode (AVC CP Only).
Telepresence Mode (CP only)	 Off - Normal conference video is sent by the Collaboration Server. Auto (Default) - If any ITP (Immersive Telepresence) endpoints are detected, ITP features are applied to the conference video for all participants. When Auto is selected, the ITP features are dynamic. If all ITP endpoints disconnect from the conference, normal conference video is resumed for all participants. ITP features are resumed for all participants should an ITP endpoint re-connects to the conference. On - ITP features are applied to the conference video for all participants regardless of whether there are ITP endpoints connected or not. Notes: This field is enabled only if the Collaboration Server system is licensed for Telepresence Mode. Telepresence Mode is unavailable in Video Switching conferences (Collaboration Server (RMX) 1500/2000/4000).
Telepresence Layout Mode (CP only)	The Telepresence Layout Mode drop-down menu enables VNOC operators and Polycom Multi Layout Applications to retrieve Telepresence Layout Mode information from the Collaboration Server. The following modes can be selected: • Manual • Continuous presence - Room Continuous Presence (Default) • Room Switch - Voice Activated Room Switching. For more information see Room Switch Telepresence Layouts. Note: This field is enabled only if the Collaboration Server system is licensed for Telepresence Mode.
Auto Scan Interval(s) (CP only)	Select the time interval, 5 - 300 seconds, that Auto Scan uses to cycle the display of participants that are not in the conference layout in the selected cell. Auto Scan is often used in conjunction with Customized Polling which allows the cyclic display to be set to a predefined order for a predefined time period.

New AVC CP Profile - Video Settings Parameters

Field/Option	Description
Auto Layout (CP only)	When selected (default), the system automatically selects the conference layout based on the number of participants currently connected to the conference. When a new video participant connects or disconnects, the conference layout automatically changes to reflect the new number of video participants.
	For more information, see Auto Layout – Default Layouts in CP Conferences.
	Clear this selection to manually select a layout for the conference.
	The default Auto Layout settings can be customized by modifying default Auto Layout system flags in the System Configuration file. For more information see, Auto Layout Configuration.
	Note: In some cases, the default layout automatically selected for the conference contains more cells than the number of connected participants, resulting in an empty cell. For example, if the number of connected participants is 4, the default layout is 2x2, but as only 3 participants are displayed in the layout (the participants do not see themselves), one cell is empty.

Auto Layout - Default Layouts in CP Conferences

Number of Video Participants	Auto Layout Default Settings
0–2	
3	
4–5	
6–7	
8-10	
11	
12+	

In layout 2+8, the two central windows display the last two speakers in the conference: the current speaker and the "previous" speaker. To minimize the changes in the layout, when a new speaker is identified the "previous" speaker is replaced by the new speaker while the current speaker remains in his/her window.



The Collaboration Server supports the VUI addition to the H.264 protocol for endpoints that transmit wide video (16:9) in standard 4SIF resolution.



When there is a change of speaker in a Continuous Presence conference, the transition is set by default to fade in the current speaker while fading out the previous speaker.

To make this transition visually pleasant, fading in the current speaker while fading out the previous speaker is done over a period of 500 milliseconds.

The Fade In/Out feature can be disabled by adding **FADE_IN_FADE_OUT** as a new flag to the System Configuration, and setting its value to **NO**.

For more information about System Flags, see Modifying System Flags.

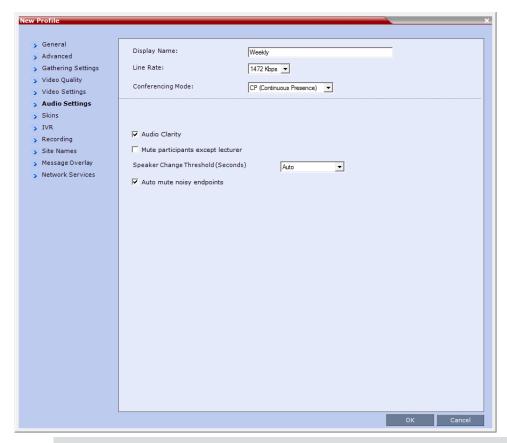
12 To select the Video Layout for the conference, click the required number of windows from the layouts bar and then select the windows array. The selected layout is displayed in the Video Layout pane.

Video Layout Options

Number of Video Windows	Avail	able Vide	o Layouts	
1				
2				
3				
4				
5+			0000	
9			0000	
10+	0000			
Overlay	0	00		
	For more information see Overlay Layouts.			

13 Click the Audio Settings tab.

The **New Profile - Audio Settings** dialog box opens.





Audio Clarity and Auto mute noisy endpoints are not supported in the RMX 1800.

14 Define the following parameters:

New AVC CP Profile - Audio Settings Parameters

Field/Option	Description
Audio Clarity	When selected, improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity.
	 The enhancement is applied to the following low bandwidth (8kHz) audio algorithms: G.729a and G.711
	 Audio Clarity is supported with MPMx and MPMRx cards only (Collaboration Server (RMX) 1500/2000/4000).
	Audio Clarity is selected by default.
	Audio Clarity cannot be selected and deselected during an ongoing conference.

New AVC CP Profile - Audio Settings Parameters

Field/Option

Description

Mute participant except lecturer

When the **Mute Participants Except Lecturer** option is enabled, the audio of all participants in the conference except for the lecturer can be automatically muted upon connection to the conference. This prevents other conference participants from accidentally interrupting the lecture, or from a noisy participant affecting the audio quality of the entire conference. Muted participants cannot unmute themselves unless they are unmuted from the Collaboration Server Web Client/RMX Manager.

You can enable or disable this option during the ongoing conference.

Notes:

- When enabled, the mute indicator on the participant endpoints are not visible because the mute participants was initiated by the MCU. Therefore, it is recommended to inform the participants that their audio is muted by using the Closed Caption or Message Overlay functions.
 - In the Collaboration Server Web Client/RMX Manager the mute by MCU indicator is listed for each muted participant in the **Audio** column in the Participants pane.
- This option can be disabled during an ongoing conference, thereby unmuting all the participants in the conference.
- If the endpoint of the designated lecturer is muted when the lecturer connects to the conference, the lecturer remains muted until the endpoint has been unmuted.
- When you replace a lecturer, the MCU automatically mutes the previous lecturer and unmutes the new lecturer.
- When you disconnect a lecturer from the conference or the lecturer leaves the conference, all participants remain muted but are able to view participants in regular video layout until the you disable the Mute Participants Except Lecturer option.
- A participant can override the Mute Participants Except Lecturer option by
 activating the Mute All Except Me option using the appropriate DTMF code,
 provided the participant has authorization for this operation in the IVR Services.
 The lecturer audio is muted and the participant audio is unmuted. You can
 reactivate the Mute Participants Except Lecturer option after a participant has
 previously activated the Mute All Except Me option. The participant is muted and
 the lecturer, if designated, is unmuted.
- In cascaded conferences, all participants (including the link participant) are muted. Only the lecturer is not muted.

Speaker Change Threshold

Indicates the amount of time a participant must speak continuously before becoming the speaker.

Select the desired threshold:

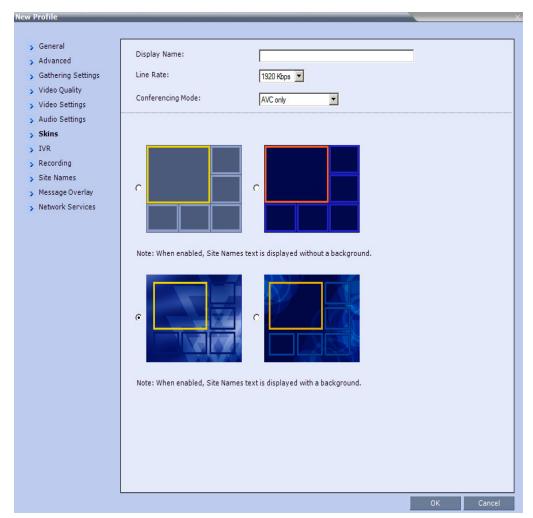
- · Auto (Default, 3 seconds)
- 1.5 seconds
- 3 seconds
- 5 seconds

New AVC CP Profile - Audio Settings Parameters

Field/Option	Description
Auto mute noisy endpoints	This option is automatically enabled in new Profiles. When enabled, the RMX can detect AVC endpoints with a noisy audio channel and automatically mute them, reducing the noise heard by other conference participants. When the auto muted endpoint becomes the "speaker" the endpoint is automatically un-muted by the system. If the speaker halts his/her conversation and the line still emits noises, the endpoint will be automatically muted again.
	Clear this check box to disable the feature.
	For more details, see Automatic Muting of Noisy Endpoints (AVC Endpoints).

15 Click the Skins tab to modify the background and frames.

The **New Profile - Skins** dialog box opens.



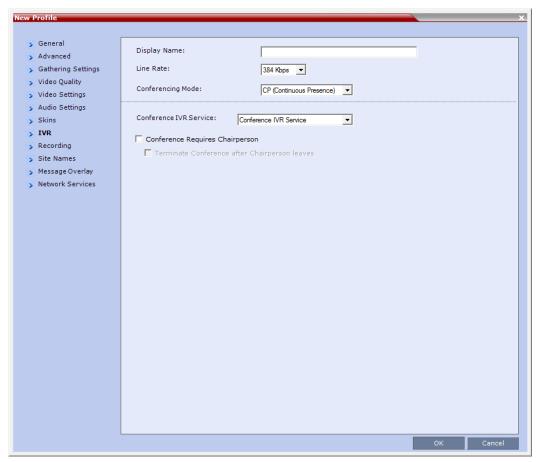
16 Select one of the Skin options.



- In Classic View (for the first two skin options) the frames fill the screen with their borders touching.
- When Telepresence Mode is enabled, the Skin options are disabled as the system uses a black background and the frames and speaker indication are disabled.

17 Click the IVR tab.

The New Profile - IVR dialog box opens.



18 If required, set the following parameters:

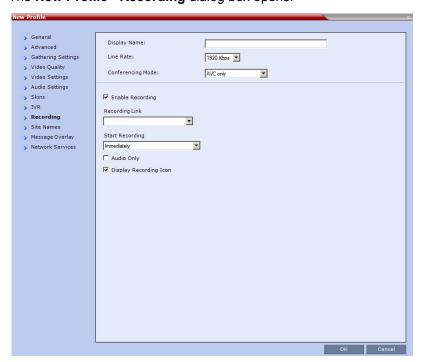
New AVC CP Profile - IVR Parameters

Field/Option	Description
Conference IVR Service	The default conference IVR Service is selected. You can select another conference IVR Service if required.

New AVC CP Profile - IVR Parameters

Field/Option	Description
Conference Requires Chairperson	Select this option to allow the conference to start only when the chairperson connects to the conference and to automatically terminate the conference when the chairperson exits. Participants who connect to the conference before the chairperson are placed on Hold and hear background music (and see the Welcome video slide). Once the conference is activated, the participants are automatically connected to the conference.
	When the check box is cleared, the conference starts when the first participant connects to it and ends at the predefined time or according to the Auto Terminate rules when enabled.
Terminate conference after chairperson leaves	Select this check box to automatically terminate the conference after the chairperson leaves. When the chairperson leaves, the Chairperson Has Left IVR message is played to all participants, at which point the conference terminates. This way an operator does not need to monitor a conference to know when to terminate it manually.
	If there is a single chairperson in the conference who is changed to a regular participant the conference will be terminated as if the chairperson left. If there is more than one chairperson, then changing one chairperson to a regular participant will not terminate the conference. It is therefore recommended that before changing a single chairperson to regular participant, another participant first be changed to chairperson.

19 Optional. Click the **Recording** tab to enable conference recording with Polycom RSS 2000/4000. The **New Profile - Recording** dialog box opens.



20 Define the following parameters:

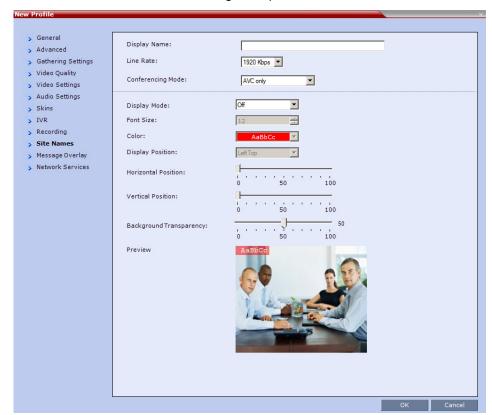
New AVC CP Profile - Recording Parameters

Parameter	Description
Enable Recording	Select this check box to enable the Recording of the conference. If no Recording Links are found, an error message is displayed.
Recording Link	Select the Recording Link to be used for conference recording. Recording Links defined on the Collaboration Server can be given a descriptive name and can be associated with a Virtual Recording Room (VRR) saved on the Polycom® RSS™ 4000 (Recording and Streaming Server). For more information see Recording Conferences
Start Recording	 Select when to start the recording: Immediately – conference recording is automatically started upon connection of the first participant. Upon Request – the operator or chairperson must initiate the recording (manual).
Audio Only	Select this option to record only the audio channel of the conference. Note: This option can be used only if there are Voice ports configured in the Video/Voice Port Configuration. For more information, see Video/Voice Port Configuration - MPMx.
Display Recording Icon	This option is automatically selected to display a Recording Indication to all conference participants informing them that the conference is being recorded. Clear the selection to prevent the display of the recording icon.



The Recording link (which is listed as a participant in the conference) does not support H.264 High Profile. If recording a conference that is set to H.264 High Profile, the Recording participant connects as Audio Only and records only the conference Audio.

21 Click the Site Names tab.



The New Profile - Site Names dialog box opens.

Using the **Site Name** dialog box, you can control the display of the site names by defining the font, size, color, background color and transparency and position within the Video Window. For a detailed description of the site names options see **Site Names Definition**.

22 Define the following parameters:

New AVC CP Profile - Site Names Parameters

Field	Description
Display Mode	 Select the display mode for the site names: Auto - Display the Site Names for 10 seconds whenever the Video Layout changes. On - Display the Site Names for the duration of the conference. Off (default) - Do not display the Site Names and all other fields in this tab are grayed and disabled
Font Size	Click the arrows to adjust the font size (in points) for the display of Site Names. Choose a Font Size that is suitable for viewing at the conference's video resolution. For example, if the resolution is CIF, a larger Font Size should be selected for easier viewing. Range: 9 - 32 points Default: 12 points

Field Description Background Color Select the color of the Site Names display text. The color and background for Site Names display text is dependent on whether a Plain Skin or a Picture Skin was selected for the conference in the Profile - Skins tab. The choices are: Plain Skin (Classic) **Picture Skin** AaBbCc Default: Default: White Text AaBbCc White Text AaBbCc No Background AaBbCc Red Background AaBbCc (For contrast, no AaBbCc background is shown as black when the text is AaBbCc white.) AaBbCc AaBbCc AaBbCc AaBbCc AaBbCc AaBbCc Note: Choose a Background Color combination that is suitable for viewing at the conference's video resolution. At low resolutions, it is recommended to select

brighter colors as dark colors may not provide for optimal viewing.

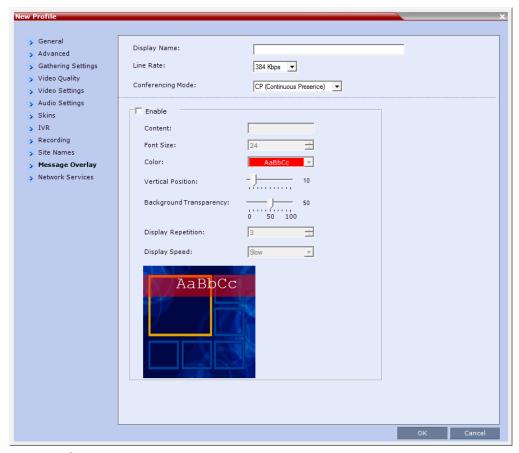
Field Description **Display Position** Select the pre-set position for the display of the Site (endpoint) Names. Selection **Site Names Position** LeftTop (Default) Site Name Display Position: Horizontal Position: Vertical Position: Top Site Name Display Position: Horizontal Position: Vertical Position: RightTop Site Name Display Position: Horizontal Position: Vertical Position: LeftMiddle Display Position: Site Name Horizontal Position: Vertical Position: RightMiddle Display Position: Site Name Horizontal Position: Vertical Position:

Field **Description Display Position** LeftBottom (cont.) Display Position: Horizontal Position: Site Name Vertical Position: **Bottom** Display Position: Horizontal Position: Vertical Position: RightBottom Display Position: Horizontal Position: Site Name Vertical Position: Custom The current endpoint (site) names display position becomes the initial position for Site Names position adjustments using the Horizontal and Vertical Position sliders. Horizontal Position Move the slider to the left to move the Note: Use of these sliders will horizontal position of the endpoint (site) set the Display Position names to the left within the video windows. selection to Custom. Move the slider to the right to adjust the horizontal position of the endpoint (site) names to the right within the video windows. Vertical Position Move the slider to the left to move the vertical position of the Site names upward within the Video Windows. Move the slider to the right to move the vertical position of the endpoint (site) names downward within the video windows.

Field	Description
Background Transparency	Move the slider to the left to decrease the transparency of the background of the endpoint (site) names text. 0 = No transparency (solid background color).
	Move the slider to the right to increase the transparency of the background of the endpoint (site) names text. 100 = Full transparency (no background color).
	Default: 50
	Note: This slider is only displayed if a Picture Skin is selected.

23 Click the Message Overlay tab.

The New Profile - Message Overlay dialog box opens.



Message Overlay enables you to send text messages to all participants during ongoing Continuous Presence conferences.

The text message is seen as part of the in the participant's video layout on the endpoint screen or desktop display.

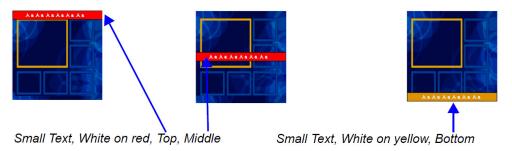
For more details, see Sending Text Messages During a Conference Using Message Overlay.

24 Define the following fields:

New AVC CP Profile - Message Overlay Parameters

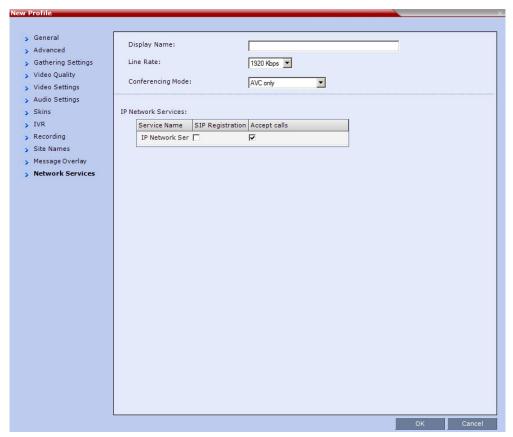
Field	Description
Enable	This option is disabled by default. Select this check box to enable Message Overlay or clear it to disable it.
Content	Enter the message text. The message text can be up to 50 Chinese characters.
Font Size	Click the arrows to adjust the font size (points) for the display of the message text. Font size range: 9 - 32 points, default: 24 points Note: In some languages, for example Russian, when a large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.
Color	From the drop-down menu select the color and background of the displayed text. The choices are: AaBbcc
Vertical Position	Move the slider to the right to move the vertical position of the displayed text downward within the Video Layout. Move the slider to the left to move the vertical position of the displayed text upward within the Video Layout. Default: Top Left (10)
Background Transparency	Move the slider to the left to decrease the transparency of the background of the message text. 0 = No transparency (solid background color). Move the slider to the right to increase the transparency of the background of the message text. 100 = Full transparency (no background color). Default: 50
Display Repetition	Click the arrows to increase or decrease the number of times that the text message display is to be repeated. Default: 3
Display Speed	Select whether the text message display is static or moving across the screen, the speed in which the text message moves: Static , Slow , Fast Default: Slow

As the fields are modified the Preview changes to show the effect of the changes. For example:



25 Click the Network Services tab.

The New Profile - Network Services dialog box opens.



Registration of conferencing entities such as ongoing conferences, Meeting Rooms, Entry Queues, SIP Factories and Gateway Sessions (Collaboration Server 1500/2000/4000) with SIP servers is done per conferencing entity. This allows better control on the number of entities that register with each SIP server. Selective registration is enabled by assigning a conference Profile in which registration is configured to the required conferencing entities. Assigning a conference Profile in which registration is not configure to conferencing entities will prevent them from registering. By default, Registration is disabled in the Conference Profile, and must be enabled in Profiles assigned to conferencing entities that require registration.

26 Define the following parameters:

New AVC CP Profile - Network Services Parameters

Parameter	Description
IP Network Services	
Service Name	This column lists all the defined Network Services, one or several depending on the system configuration.
SIP Registration	To register the conferencing entity to which this profile is assigned with the SIP Server of the selected Network Service, click the check box of that Network Service in this column.
	When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register with an URL derived from its own signaling address. In Collaboration Server 1500/2000/4000, this unique URL replaces the non-unique URL, dummy_tester, used in previous versions.
Accept Calls	To prevent dial in participants from connecting to a conferencing entity when connecting via a Network Service, clear the check box of the Network Service from which calls cannot connect to the conference.

27 Click **OK** to complete the Profile definition.

A new Profile is created and added to the Conference Profiles list.

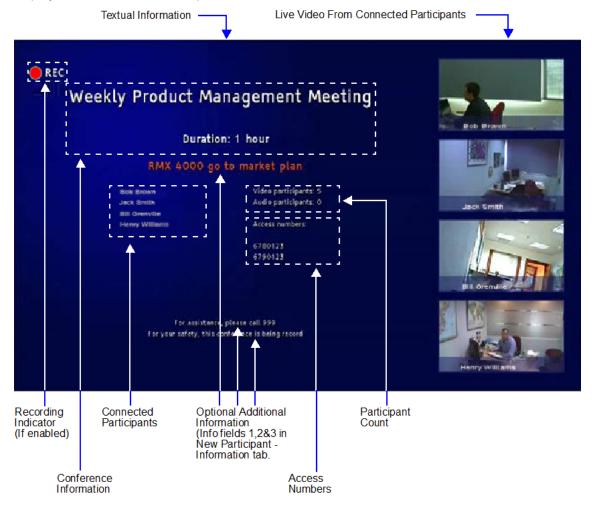
Additional Information for Setting CP Profiles

This section includes detailed explanation of various CP Profile settings:

- Gathering Phase
- Overlay Layouts
- Site Names Definition
- Sending Text Messages During a Conference Using Message Overlay
- Selecting the Chinese Font for Text Display

Gathering Phase

The Gathering Phase of an AVC (CP only) conference is the time period during which participants are connecting to a conference. During the *Gathering Phase*, a mix of live video from connected endpoints is combined with both static and variable textual information about the conference into a slide which is displayed on all connected endpoints.



During the Gathering Phase, the audio of all participants can be heard, and the video of active speakers is displayed in the video windows as they begin talking.

All connected participants are kept informed about the current conference status including names of connected participants, participant count, participant type (video/audio) etc.

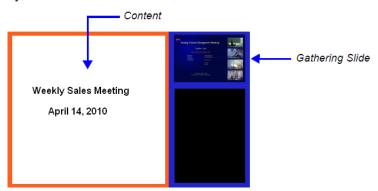
Gathering Phase Guidelines

- Gathering Phase is only available in AVC only (CP only) conferences. It is not supported in Video Switching conferences and SVC Only conferences.
- The Gathering Phase slide can be displayed at any time during the conference by entering the Show Participants DTMF code, *88.

Note: When the display of the Gathering Phase slide is removed, the message overlay text is also removed.

- The names of the first eight participants to connect are displayed. If eight or more participants connect, the 8th row displays "...".
- Static text in the Gathering Phase slide such as the field headings: Organizer, Duration, Video/Audio Participants, Access Number, IP are always displayed in the language as configured in the Polycom Virtual Meeting Rooms Add-in for Microsoft Outlook. The following languages are supported:
 - > English
 - French
 - German
 - International Spanish
 - Korean
 - Japanese
 - > Simplified Chinese
- Dynamic text in the Gathering Phase slide such as the meeting name, participants' names, access numbers and the additional information entered in the Info1/2/3 fields of the Gathering Settings tab of the conference Profile are displayed in the language of the meeting invitation.
- The language of a Gathering Phase slide of a conference configured to include a Gathering Phase
 that is not launched by the Polycom Conferencing Add-in for Microsoft Outlook is configured by the
 administrator. Using the Collaboration Server Web Client, the administrator selects the language for
 the Gathering Phase slide. The language selected can be different to that of the Collaboration Server
 Web Client used by the administrator to perform the configuration.

Content can be sent during the Gathering Phase. The content is displayed in the large video window
of the participant's layout while the Gathering slide is displayed in a smaller video window in the
layout.



Gathering is not supported in Cascading Conferences.

Gathering Phase Duration

The duration of the Gathering Phase can be customized by the administrator so that it is long enough to be viewed by most connected participants yet short enough so as not to over extend into the scheduled conferencing time.

The Gathering Phase duration is configured for the Collaboration Server, by the following System Flags in system.cfg in the **Setup >System Configuration**:

CONF_GATHERING_DURATION_SECONDS

Range: 0 - 3600 seconds
Default: 180 seconds

The Gathering Phase duration of the conference is measured from the scheduled start time of the conference.

Example: If the value of the flag is set to **180**, the Gathering slide is displayed for three minutes to all participants starting at the conference Start Time, and ending three minutes after the conference Start Time.

For participants who connect before Start Time, the Gathering slide is displayed from the time of connection until the end of the Gathering duration period.

• PARTY_GATHERING_DURATION_SECONDS

Range: 0 - 3600 seconds

Default: 15 seconds

The value of this flag determines the duration of the display of the Gathering slide for participants that connect to the conference after the conference Start Time.

Participants connecting to the conference very close to of the end of the Gathering Phase (when there are fewer seconds left to the end of the Gathering Phase than specified by the value of the flag) have the Gathering slide displayed for the time specified by the value of the flag.

Example: If the value of the flag is set to **15**, the Gathering Phase slide is displayed to the participant for 15 seconds.

Enabling the Gathering Phase Display

The Gathering Phase is enabled for per conference in the Conference Profile. The profile also includes the dial-in numbers and the optional additional information to display on the slide.

Conferences that are configured to include a Gathering Phase that are not launched by the Polycom Conferencing Add-in for Microsoft Outlook need the following information to be entered via the **New Profile** or **Profile Properties** — **Gathering Settings** dialog box:

- Display Name (Optional, the Meeting Name is used if left blank.)
- Displayed Language
- Access Number 1 / 2 (Optional.)
- Additional Information (Optional free text)
 - ➤ Info 1
 - ➤ Info 2
 - ➤ Info 3

Conferences launched by the Polycom Conferencing Add-in for Microsoft Outlook receive this information from the meeting invitation.

For more information see Defining New Profiles.

Overlay Layouts

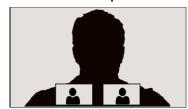
In Overlay Layouts additional participant endpoints can be displayed over the full screen display of the conference speaker.

The following Overlay Layouts are available for use in CP Conferences:

1Standalone Endpoint



2 Standalone Endpoints

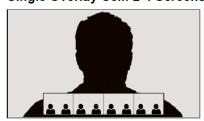


3 Standalone Endpoints



Although the following Overlay Layout is included in the **Profiles - Video Settings** dialog box, it is not available for use in any Conferencing Mode and is only available when included in the Polycom® Multipoint Layout (MLA) application:

Single Overlay Cell: 2-4 Screens





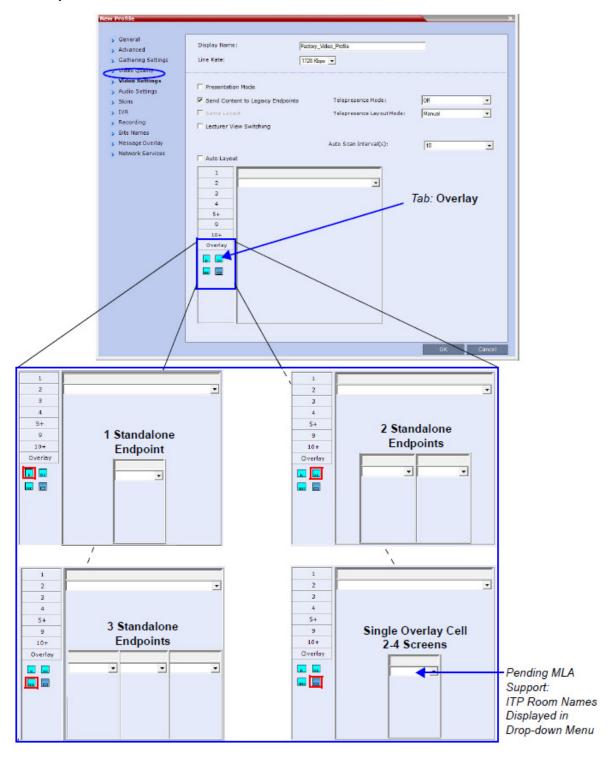
These Overlay Layouts will only be available in ITP (Telepresence) conferences when support for Overlay Layouts is included in the Polycom® Multipoint Layout (MLA) application.

Guidelines for using the Overlay Layouts

- The Overlay Layouts are supported:
 - In CP Conferencing Mode only.
 - > With ITP, non-ITP and CTS endpoints used only as standard endpoints.
 - > With both new and classic Skins in Collaboration Server CP mode.
- Overlay Layouts are not supported in ITP conferences as they are not supported by the MLA application.
- The Overlay Layouts are 20% of the height of the endpoint display and are supported on endpoints of both 16:9 and 4:3 aspect ratios.
- Overlay Layouts are recommended for use with high resolution endpoints.
- Overlay Layouts are not selected as defaults by the system and are not included in the Auto Layout settings.
- Message Overlay is not affected by the use of Overlay Layouts and is displayed on top of the video layouts.
- Site Names are displayed for all cells. Because the smaller cells are located at the bottom of the large cell, when enabling Site Names it is advisable not to locate the Site Name at the bottom of the cells.
- Standalone Endpoint Cells are displayed each with a border. For all Overlay Layouts, border color is dependent on the selected Skin.
- System behavior for Video Forcing and Personal Layout Control when using the Overlay Layouts during an ongoing conference is the same as for other video layouts.
- Overlay Layouts are only available for selection for the Conference Layout and are not available for selection for Personal Layout.
- During an ongoing conference you cannot select the Overlay Layouts via PCM or Click&View.
- PCM menus can be used when the Overlay Layouts are active, and they are displayed as the top layer.

Selecting the Overlay Layouts

The Overlay Layouts are selected in the **New Profile - Video Settings** dialog box, in the **Overlay** tab of the Video Layout tree.



Site Names Definition

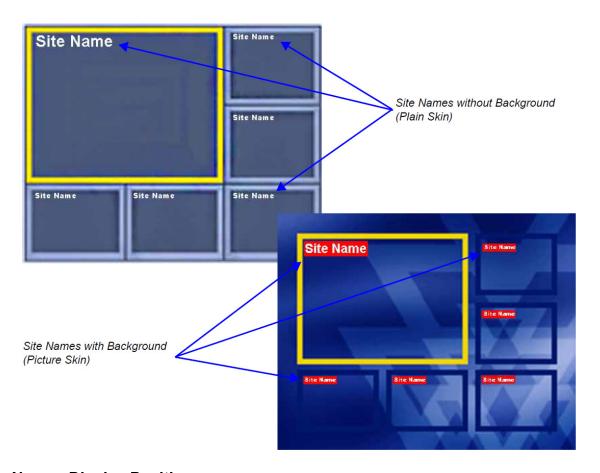


The Site Names feature is not supported in the RMX 1800.

You can control the display of the site names by defining the font, size, color, background color and transparency and position within the video window in the **Profile - Site Name** dialog box.

Guidelines

- Site Names display is Off by default in a new profile.
- Site Names can be enabled to function in one of two modes:
 - > Auto Site names are displayed for 10 seconds whenever the conference layout changes.
 - ➤ On Site names are displayed for the duration of the conference.
- During the display of the site names, the video frame rate is slightly reduced
- Site Names display is not available for Video Switching (VSW) conferences (Collaboration Server (RMX) 1500/2000/4000.
- Site Names display characteristics (position, size, color) can by modified during an ongoing conference using the **Conference Properties Site Names** dialog box. Changes are immediately visible to all participants.
- Site Names display text and background color is dependent on the Skin selected for the conference:
 - > Plain Skins Site Names text is displayed without a background.
 - > Picture Skins Site Names text is displayed with a background.



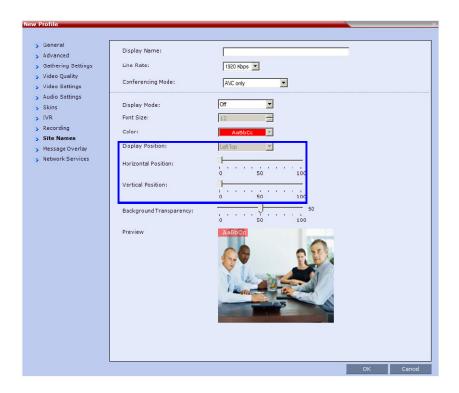
Site Names Display Position

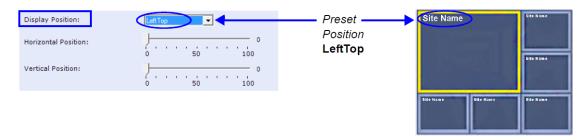


Site Names, Horizontal and Vertical Position and Background Transparency are not supported in the RMX 1800.

The position of the Site Names displayed during the conference is controlled in the **Profile - Site Names** tab. The following options can be used to define the display position:

- Display Position drop-down menu To select a preset position.
- Horizontal Position and Vertical Position sliders To move them to customize the preset position.
 Dragging the sliders sets the Display Position drop-down menu field value to Custom.
- Selecting Custom in Display Position drop-down menu. When selected, the current position becomes the initial position for position adjustments and then using the Horizontal and Vertical Position sliders to define the exact position.



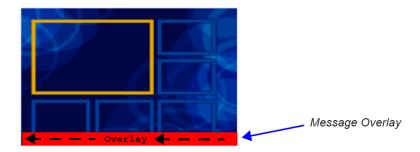


The adjusted position of the Site Names can be viewed in the **Preview**.

Sending Text Messages During a Conference Using Message Overlay

The Message Overlay option in the Conference Profile allows the operator or administrator to send text messages to all participants during an ongoing conference.

The text message is seen as part of the participant's video layout on the endpoint screen or desktop display.



Guidelines

- Text messaging using Message Overlay is supported in:
 - MPMx and MPMRx Card Configuration Modes
 - > Continuous Presence (CP) conferences
 - Same Layout mode
 - Encrypted conferences
 - > With Unicode or ASCII characters
- Text messages using Message Overlay cannot be displayed:
 - ➤ In Video Switching (VSW) conferences (Collaboration Server 1500/2000/4000).
 - In Lecture Mode
 - When the PCM menu is active
 - > On endpoints that have their video suspended
- Text messaging using Messages Overlay can be enabled, disabled or modified (content and display parameters) during the ongoing conference.
- The number of characters for each language can vary due to the type of font used, for example, the available number of characters for Chinese is 18, while for English and Russian it is 48.
 - In some languages, for example Russian, when large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.
- Changes to the Message Overlay Content or display characteristics (position, size, color and speed) are immediately visible to all participants. When there is a current Message Overlay:
 - > The current message is stopped immediately, even it has not completed all of its repetitions.
 - The Display Repetition count is reset to 1.
 - > The new message content is displayed < Display Repetition > times or until it is stopped and replaced by another content change.
- If during the ongoing conference the Show Number of Participants DTMF option (default DTMF *88) is used, when the displayed number of participants is removed, the message overlay text is also removed.

- The text messages cannot be sent via the Content channel.
- Message Overlay text settings are not saved in the Conference Template when saving an ongoing conference as a Conference Template.
- Text messages can also be sent to individual or several participants during the ongoing conferences.
 For more details, see the Polycom Real Presence Collaboration Server (RMX) 1500/1800/2000/4000
 Getting Started Guide, Sending Messages to Selected Participants Using Message Overlay
 (AVC-based Conferences).

For a detailed description of all the Message Overlay parameters, see New AVC CP Profile - Message Overlay Parameters.

Selecting the Chinese Font for Text Display

When using the RMX Web Client or the RMX Manager in Chinese (either Simplified Chinese or Traditional Chinese is selected as an available language in the **Setup > Customize Display Settings > Multilingual Setting**, you can select one of several Chinese fonts for use when sending text over video. The font is used to display text for the following:

- · Display of Site Names
- Test messages sent using Message Overlay
- Text displayed on the Gathering slide when Chinese is selected as the display language

Selecting the Chinese Font

The Chinese fonts can be selected in the CP Conference **Profile - Advanced** dialog box only.



The following Chinese fonts are available for selection:

- Heiti (Default)
- Songti
- Kaiti
- Weibei

The Chinese font cannot be changed during an existing conference. It can only be modified in the conference profile.

A participant moved to another conference will be shown the font used by the new conference.

Defining an AVC Video Switching Conference Profile

An AVC Video Switching-enabled Profile must be created prior to running Video Switching conferences. This profile can be assigned to Meeting Rooms, conferences, reservations and Entry Queues

To connect to a Video Switching conference via an Entry Queue, the Entry Queue must be Video Switching enabled and must be set to the same line rate as the target conference. It is recommended to use the same Profile for both the target conference and Entry Queue.

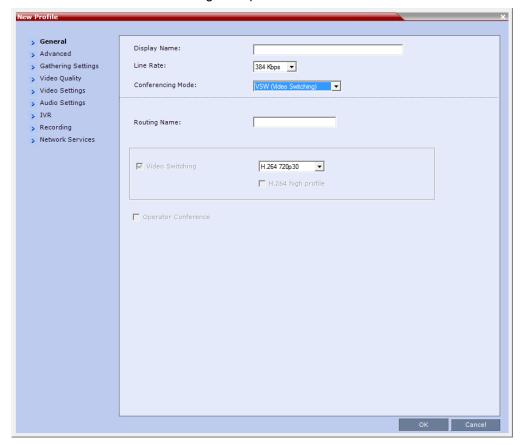
Video Switching conferencing mode is unavailable to ISDN participants.

When the Conferencing Mode is set to Video Switching, only the tabs and fields relevant to Video Switching conferences are displayed and enabled.

To Create a Video Switching Profile:

- 1 In the RMX Management pane, click Conference Profiles.
- 2 In the Conference Profiles pane, click the New Profile button.

The **New Profile – General** dialog box opens.



3 Define the **New Profile - General** parameters:

New AVC VSW Profile - General Parameters

Field/Option	Description	
Display Name	 Enter a unique Profile name, as follows: English text uses ASCII encoding and can contain the most characters (lenvaries according to the field). European and Latin text length is approximately half the length of the maximum. Asian text length is approximately one third of the length of the maximum. It is recommended to use a name that includes the Profile type, such as Week Video Switching conference. Note: This field is displayed in all tabs. 	
Line Rate	Select the conference bit rate. The line rate represents the combined video, audio and Content rate. When defining a VSW profile, select a line rate that all connecting participants can use. Participants that their endpoint or network that do not support this line rate cannot connect to the conference or will connect as Audio Only (if resources were designated as Voice ports). If a high definition resolution will be selected for the conference video, make sure that the selected line rate is higher than the minimum line rate threshold defined in the flag HD_THRESHOLD_BITRATE for Video Switching conferences. The default setting is 384 Kbps. Note: This field is displayed in all tabs.	
Conferencing Mode	Select VSW (Video Switching) to define a VSW conference Profile. Note: This field is displayed in all tabs.	
Routing Name	 Enter the Profile name using ASCII characters set. The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows: If an all ASCII text is entered in Display Name, it is used also as the Routing Name. If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name. 	

New AVC VSW Profile - General Parameters (Continued)

Field/Option	Description	
Video Switching	This check box is automatically selected when the Conferencing Mode is set to Video Switching.	
	Select the video protocol and resolution for the conference:	
	• H.264 1080p60	
	• H.264 1080p30	
	• H.264 720p60	
	• H.264 720p30	
	• H.264 SD 30	
	• H.264 CIF	
	• H.263 CIF	
	• H.261 CIF	
	All participants must connect at the same line rate and use the same video resolution. Participants with endpoints that do not support the selected line rate and resolution will connect as secondary (audio only).	
	For more information, see Video Switching (VSW) Conferencing.	
H.264 High Profile	Select this check box to enable the use of H.264 High Profile in Video Switching conferences.	
	The High Profile check box is only displayed if MPMx cards are installed in the RMX. By default the High Profile check box is not selected.	
	If H.264 is not the selected video protocol the check box is inactive (grayed out). For more information, see H.264 High Profile Support in Video Switching Conferences.	
Operator Conference	This option is unavailable and disabled in VSW Conferencing Mode.	



Selecting a new conference line rate lower than the initial line rate selected for the conference (for example, changing from 4096 kbps to 1532 kbps) may result in system reverting to the default resolution for that line rate (for example, 720p instead of 1080p). You may need to select the required resolution again, provided the selected line rate is higher than the minimum threshold line rate defined for that resolution in the system configuration. For more details, see Minimum Threshold Line Rate System Flags below.

4 Define the various Profile parameters for a Video Switching conference. As it is an AVC -bases conferencing mode, many of the fields and options are identical to the CP Profile. For more information, see Defining AVC CP Conferencing Profiles.

The following AVC-based conferencing options are **not available** in VSW conferences:

- Operator Conference
- Gathering Phase
- Video Quality Send Content To Legacy Endpoints
- > Video Settings:
 - Presentation Mode
 - ♦ Auto Layout/Same Layout (only full screen, 1x1 layout display is available)

- Auto Scan
- Skins
- Site Names
- Message Overlay
- 5 Click OK.

H.264 High Profile Support in Video Switching Conferences

Beginning with Version 7.6, the H.264 High Profile video protocol is supported in Video Switching (VSW) conferences.

Guidelines

- H.264 High Profile is supported in VSW conferences in H.323 and SIP networking environments only
- For H.264 High Profile-enabled VSW conferences, all endpoints connecting to the conference must support High Profile and connect to the VSW conference at the exact line rate and exact resolution defined for the conference. Endpoints that do not meet these requirements are connected as Secondary (audio only).
- For H.264 Base Profile VSW conferences, both High Profile and Base Profile supporting endpoints connect using the H.264 Base Profile.
 - > Endpoints that do not support the exact conference line rate are disconnected.
 - > Endpoints that do not support the exact video settings such as protocol and resolution defined for the conference will be connected as Secondary (audio only).

Minimum Threshold Line Rate System Flags

The following table lists the System Flags that control the minimum line rate threshold for the various resolutions available for High Profile-enabled VSW conferences.

These system flags must be manually added to the **Setup menu > System Configuration** before you can update their values. For more information see the <u>Modifying System Flags</u>.

System Flags - Minimum Threshold Line Rates

Flag Name	Minimum Threshold Line Rate (Kbps)
VSW_CIF_HP_THRESHOLD_BITRATE	64
VSW_ SD _HP_THRESHOLD_BITRATE	128
VSW_ HD720p30 _HP_THRESHOLD_BITRATE	512
VSW_ HD720p50-60 _HP_THRESHOLD_BITRATE	832
VSW_ HD1080 p_HP_THRESHOLD_BITRATE	1024
VSW_ HD1080p60 _HP_THRESHOLD_BITRATE	1024
VSW_HD_1080p60_BL_THRESHOLD_BITRATE	1728

- Line rate and resolution combinations are checked for validity. If the selected line rate is below the minimum line rate threshold required for the selected resolution, the line rate is automatically adjusted to the minimum line rate threshold value for the selected resolution.
- The value of the SUPPORT_HIGH_PROFILE system flag (used for CP conferences) has no effect on VSW conferences.

Defining SVC and Mixed CP and SVC Conference Profiles



Although SVC Conferencing Mode options are available in Conference Profiles, it is advised that they not be used with Version 8.1.4.J.

Defining SVC Conference Profiles

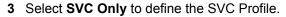
The SVC conference Profile definition is started by selecting SVC as the Conferencing Mode. The dialog boxes and their options change as the conference behavior and the MCU video processing change. For example, site name display is performed and controlled by the SVC endpoint and not by the MCU as in CP conferences.

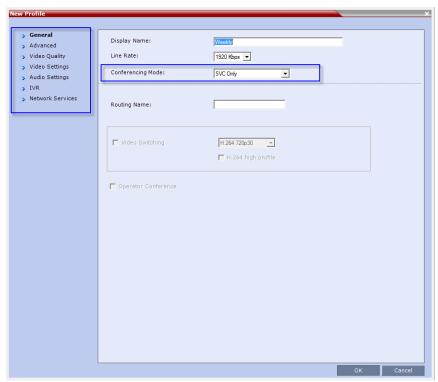
To define SVC Only Profile:

- 1 In the RMX Management pane, click Conference Profiles.
- 2 In the Conference Profiles pane, click the New Profile button.

The New Profile - General dialog box opens.

By default, the Conferencing Mode is set to CP.





The profile tabs and options change accordingly and only supported options are available for selection. Unsupported options are disabled (grayed out).

4 Define the Profile name and, if required, the **Profile - General** parameters:

New SVC Profile - General Parameters

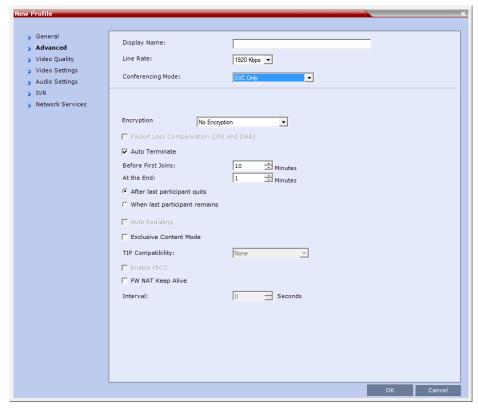
Field/Option	Description	
Display Name	 Enter a unique Profile name, as follows: English text uses ASCII encoding and can contain the most characters (length varies according to the field). European and Latin text length is approximately half the length of the maximum. Asian text length is approximately one third of the length of the maximum. This is the only parameter that must be defined when creating a new profile. Note: This field is displayed in all tabs. 	
Line Rate	Select the conference bit rate. The line rate represents the combined video, audio and Content rate. The default setting for SVC Only conferences is 1920 kbps. Note: This field is displayed in all tabs.	

New SVC Profile - General Parameters

Field/Option	Description
Routing Name	 Enter the Profile name using ASCII characters set. You can define the Routing Name or it can be automatically generated by the system if no Routing Name is entered as follows: If an all ASCII text is entered in Display Name, it is used also as the Routing Name. If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.

5 Click the Advanced tab.

The **New Profile – Advanced** dialog box opens.



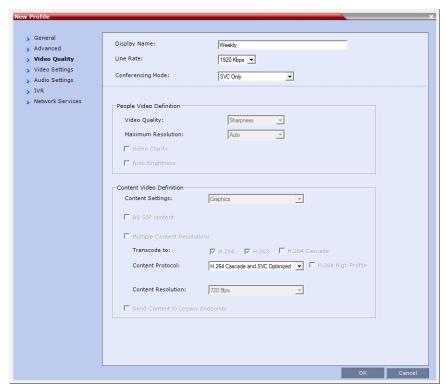
6 Define the following supported parameters:

New SVC Profile - Advanced Parameters

Field/Option	Description	
Encryption	 Select the Encryption option for the conference: Encrypt All - Encryption is enabled for the conference and all conference participants must be encrypted. No Encryption - Encryption is disabled for the conference. Encrypt when Possible - enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. For connection guidelines see Mixing Encrypted and Non-encrypted Endpoints in one Conference. For more information, see Packet Loss Compensation (LPR and DBA) AVC CP Conferences. 	
Auto Terminate	 When selected (default), the conference automatically ends when the termination conditions are met: Before First Joins — No participant has connected to a conference during the n minutes after it started. Default idle time is 10 minutes. At the End - After Last participant Quits — All the participants have disconnected from the conference and the conference is idle (empty) for the predefined time period. Default idle time is 1 minute. At the End - When Last Participant Remains — Only one participant is still connected to the conference for the predefined time period (excluding the recording link which is not considered a participant when this option is selected). It is not recommended to select this option for SVC Conferences. Default idle time is 1 minute. 	
Exclusive Content Mode	When selected, Content broadcasting is limited to one participant preventing other participants from interrupting the Content broadcasting while it is active. For more details, see	
FW NAT Keep Alive	When selected, a FW NAT Keep Alive message is sent at an interval defined in the field below the check box.	
Interval	The time in seconds between FW NAT Keep Alive messages.	

7 Click the Video Quality tab.

The New Profile - Video Quality dialog box opens.



8 In SVC Conferencing Mode, the video and Content sharing parameters cannot be modified and they are set to the following parameters:

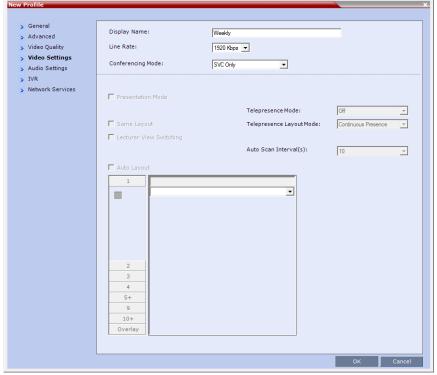
New SVC Profile - Video Quality Parameters

Field/Option	Description	
People Video Definition	on	
Video Quality	Only Sharpness is available in SVC Conferencing Mode. The MCU sends the video stream in the resolution required by the endpoint.	
Maximum Resolution	Only Auto is available in SVC Conferencing Mode. The MCU sends the video stream in the resolution required by the endpoint.	
Content Video Definition		
Content Settings	Only Graphics is available in SVC Conferencing Mode for transmission of Content. It offers the basic mode, intended for normal graphics. For more information, see Video Preview (AVC Participants Only).	

New SVC Profile - Video Quality Parameters

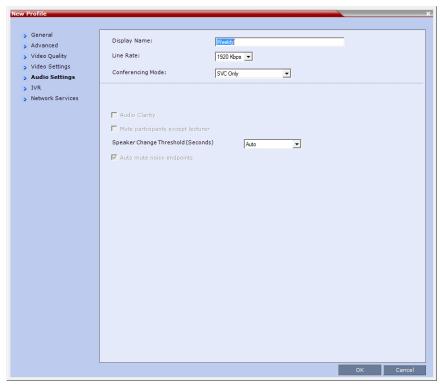
Field/Option	Description
Content Protocol	H.264 Cascade and SVC Optimized is the only available Content Protocol for content sharing during SVC-based conferences. In this mode, all <i>Content</i> is shared using the <i>H.264</i> content protocol and all endpoints must use the set video resolution and frame rate (720p 5fps). Endpoints that do not support these settings cannot
	share content.

9 Click the Video Settings tab.



In SVC conferences, each endpoint determines its own video layout and there is no conference level layout selected. Therefore, all the Video Settings parameters are disabled.

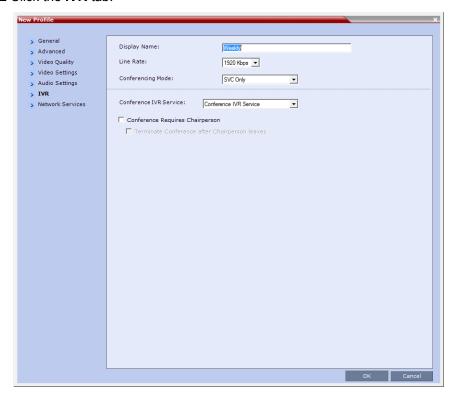
10 Click the Audio Settings tab.



11 If required, define the **Speaker Change Threshold**: Auto (Default, 3 seconds), 1.5.3.5.

It indicates the amount of time a participant must speak continuously before becoming the speaker.

12 Click the IVR tab.



13 If required, set the following parameters:

New SVC Profile - IVR Parameters

Field/Option	Description	
Conference IVR Service	The default conference IVR Service is selected. You can select another conference IVR Service if required.	
Conference Requires Chairperson	Select this option to allow the conference to start only when the chairperson connects to the conference and to automatically terminate the conference when the chairperson exits. Participants who connect to the conference before the chairperson are placed on Hold and hear background music (and see the Welcome video slide). Once the conference is activated, the participants are automatically connected to the conference.	
	When the check box is cleared, the conference starts when the first participant connects to it and ends at the predefined time or according to the Auto Terminate rules when enabled.	
Terminate conference after chairperson leaves		

The following IVR features are not supported during SVC conferences:

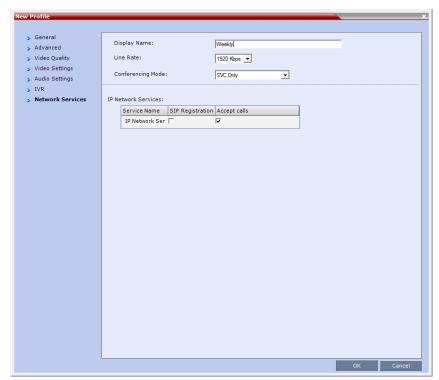
- > Roll Call
- > Invite Participants
- > Entry and Exit tones
- Click & View
- ➤ PCM



On the RMX 1800, Roll Call, Entry and Exit tones are supported in SVC-only conferences.

14 Click the Network Services tab.

The New Profile - Network Services tab opens.



Registration of conferencing entities such as ongoing conferences, Meeting Rooms, and SIP Factories with SIP servers is done per conferencing entity. This allows better control of the number of entities that register with each SIP server. Selective registration is enabled by assigning a conference Profile in which registration is configured for the required conferencing entities. Assigning a conference Profile in which registration is not configure for conferencing entities will prevent them from registering. By default, Registration is disabled in the Conference Profile, and must be enabled in Profiles assigned to conferencing entities that require registration.

15 Define the following parameters:

New SVC Profile - Network Services Parameters

Parameter	Description	
IP Network Services		
Service Name	This column lists all the defined Network Services, one or several depending on the system configuration.	
SIP Registration	To register the conferencing entity to which this profile is assigned with the SIP Server of the selected Network Service, click the check box of that Network Service in this column. When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register	
	with an URL derived from its own signaling address.	

New SVC Profile - Network Services Parameters

Parameter	Description	
Accept Calls	To prevent dial in participants from connecting to a conferencing entity when connecting via a Network Service, clear the check box of the Network Service from which calls cannot connect to the conference.	

16 Click **OK** to complete the Profile definition.

A new Profile is created and added to the Conference Profiles list.

Defining Mixed CP and SVC Conferencing Profiles



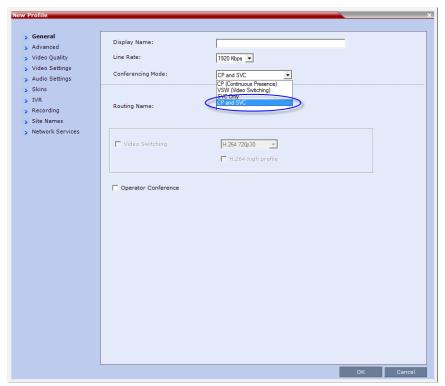
Although SVC Conferencing Mode options are available in Conference Profiles, it is advised that they not be used with Version 8.1.4.J.

The mixed CP and SVC Profile is based on the CP Profile with a few of the CP options disabled for compatibility between AVC and SVC protocols and to enable the media conversion between these two modes. The **Gathering Settings** and the **Message Overlay** options are unavailable in this Conferencing Mode

In a mixed CP and SVC conference, the Chairperson can be either an AVC-enabled or SVC-enabled endpoint.

To configure a mixed AVC and SVC conference:

- 1 In the RMX Management pane, click Conference Profiles.
- 2 In the Conference Profiles pane, click the New Profile button.
 The New Profile General dialog box is displayed.
- 3 In the Conferencing Mode list, select CP and SVC to define a mixed AVC and SVC conference.



Using the various Profile tabs, you can define the following profile parameters:

- CP and SVC Profile Advanced parameters these parameters are the same as for CP conferences. For details, see New AVC CP Profile - Advanced Parameters.
- CP and SVC Profile Video Quality parameters to enable the sharing of video between SVC and AVC, the common denominator parameters (in this conference, the SVC parameters) are selected for the conference. For more details, see New SVC Profile - Video Quality Parameters.
- CP and SVC Profile Video Settings parameters the video layout parameters apply only to the AVC-enabled endpoints and do not apply to SVC-enabled endpoints as the SVC endpoints generate their own layout. Options that are not supported in SVC conferencing are disabled in this dialog box, for example, Telepresence Mode. For more details, see New AVC CP Profile - Video Settings Parameters.
- CP and SVC Profile Audio Settings parameters options that are not supported in SVC conferencing are disabled in this dialog box. For more details, see New AVC CP Profile - Audio Settings Parameters.
- CP and SVC Profile Skins parameters the display of a video skin applies only to the AVC-enabled endpoints and do not apply to SVC-enabled endpoints as the SVC endpoints generate their own layout.
- CP and SVC Profile IVR parameters to enable the same IVR behavior and DTMF usage for SVC and AVC, the common denominator parameters (in this conference, the SVC parameters) are selected for the conference. For more details, see New SVC Profile - IVR Parameters.
- CP and SVC Profile Recording parameters these parameters are the same as for CP conferences as the recording is done in AVC format. For details, see New AVC CP Profile - Recording Parameters.
- CP and SVC Profile Site Names parameters these parameters are the same as for CP conferences as they apply the AVC-enabled endpoints. SVC-enabled endpoints generate the site name display independent of the MCU. For details, see New AVC CP Profile Site Names Parameters.
- CP and SVC Profile Network Services parameters these parameters are the same as for CP and SVC conferences . For details, see New AVC CP Profile Network Services Parameters.

Video Protocols and Resolution Configuration for CP Conferencing

Video Resolutions in AVC-based CP Conferencing



The following video resolution information applies to AVC CP Conferencing Mode. For a description of resolutions for SVC Conferencing Mode see Defining SVC Conference Profiles.

The RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 always attempts to connect to endpoints at the highest line rate defined for the conference. If the connection cannot be established using the conference line rate, the Collaboration Server attempts to connect at the next highest line rate at its highest supported resolution.

Depending on the line rate, the Collaboration Server sends video at the best possible resolution supported by the endpoint regardless of the resolution received from the endpoint.

The video resolution is also defined by the Video Quality settings in the Profile.

- Motion, when selected, results in lower video resolution at higher frame rates (30 fps to 60 fps).
- **Sharpness**, when selected, results in higher video resolution at lower frame rate (30 fps and lower). However, it can also be sent in 1080P 60fps.

The combination of frame rate and resolution affects the number of video resources required on the MCU to support the call.

The following resolutions are supported:

• CIF	352 x 288 pixels	at 30 or 60 fps
• SD	720 x 576 pixels	at 30 or 60 fps
• HD 720p	1280 x 720 pixels	at 30 or 60 fps
• HD 1080p	1920 x 1080 pixels	at 30 fps
• HD 1080p	1920 x 1080 pixels	at 60 fps (Symmetric in Motion, a-symmetric in Sharpness

Video Display with CIF, SD and HD Video Connections

Although any combination of CIF, SD and HD connections is supported in all CP conferences, the following rules apply:

- In a 1X1 Video Layout:
 - > **SD:** If the speaker transmits CIF, the MCU will send CIF to all participants, including the SD participants. In any other layout the MCU will transmit to each participant at the participant's sending resolution.
 - ➤ HD: The MCU transmits speaker resolution (including input from HD participants) at up to SD resolution. If 1x1 is the requested layout for the entire duration of the conference, set the conference to HD Video Switching mode.
- In asymmetrical Video Layouts:
 - > **SD:** A participant in the large frame that sends CIF is displayed in CIF.
 - > HD: Where participants' video windows are different sizes, the Collaboration Server transmits HD and receives SD or lower resolutions.
- In panoramic Video Layouts:
 - > **SD**: Participants that send CIF also receive CIF.
 - ➤ **HD**: the Collaboration Server transmits HD and receives SD or lower resolutions, the Collaboration Server scales images from SD to HD resolution.

H.264 High Profile Support in CP Conferences

The H.264 High Profile is a new addition to the H.264 video protocol suite. It uses the most efficient video data compression algorithms to even further reduce bandwidth requirements for video data streams.

Video quality is maintained at bit rates that are up to 50% lower than previously required. For example, a 512Kbps call will have the video quality of a 1Mbps HD call while a 1Mbps HD call has higher video quality at the same (1Mbps) bit rate.



H.264 High-Profile should be used when all or most endpoints support it.

H.264 High Profile Guidelines

- H.264 High Profile is supported in H.323, and SIP and ISDN networking environments.
- H.264 High Profile is supported in Continuous Presence conferences at all bit rates, video resolutions and layouts.
- H.264 High Profile is the first protocol declared by the Collaboration Server, to ensure that endpoints that support the protocol will connect using it.
 - Setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the H.264 High Profile.
- For monitoring purposes, the Collaboration Server and endpoint H.264 High Profile capability is listed in the Participant Properties - H.245 and SDP tabs for H.323 participants and SIP participants respectively.

For more information see Monitoring IP Participants.

- H.264 High Profile is not supported:
 - For Content Sharing with MPMx cards
 - With Video Preview

HD1080p60 Resolution Guidelines

HD1080p60 resolution is supported in Continuous Presence (CP) mode:

- With MPMx media cards:
 - > Asymmetrically: The Collaboration Server receives HD720p60 and sends HD1080p60.
 - In both Video Quality modes (**Motion** or **Sharpness**).
 - With line rates between 2Mbps and up to 4 Mbps (the maximum line rate available for CP conferences).
- With MPMRx media cards:
 - Symmetrically: The Collaboration Server receives and sends HD1080p60.
 - > With Video Quality mode set to Motion.
 - For H.323 and SIP participants.
 - > At line rates up to 4Mbps.

HD1080p60 resolution is supported in Video Switching (VSW) mode:

- > At bit rates of up to 6Mbps.
- ➤ HD1080p60 is supported symmetrically: The RMX receives and sends HD1080p60.

HD1080p60 resolution is not supported:

- > For ISDN participants.
- For Content sharing.
- With RTV video protocol.

HD1080p60 resolution is not supported symmetrically:

- ➤ In 1X1 layouts, including 1X1 layouts in Telepresence Mode. Instead, the Collaboration Server transmits the current speaker endpoint's video resolution and frames per second.
- In TIP environments.

In Telepresence environments the RMX receives HD720p60 and sends HD1080p60 to all endpoints except for those with 1x1 Video Layouts, which receive the same resolution and frame rate from the RMX as they send. TIP endpoints are not supported.

PAL endpoints are supported at a frame rate of 50 fps.

CP Conferencing with H.263 4CIF

The video resolution of 4CIF in H.263 endpoints is only supported for conferences in which the video quality is set to sharpness and for line rates of 384 Kbps to 1920 Kbps as shown in the following table.

Video Quality vs. Line Rate

Endpoint Line Rate Kbps	Video Quality			
	Motion		Sharpness	
	Resolution	Frame Rate	Resolution	Frame Rate
128	QCIF	30	CIF	30
256	CIF	30	CIF	30
384 - 1920+	CIF	30	4CIF	15

Video Quality vs. Line Rate

Endpoint Line Rate Kbps	Video Quality		
Enupoint Line Rate Rups	Resolution	Frame Rate	
128	CIF	30	
256	CIF	30	
384 - 1920+	4CIF	15	

The Collaboration Server Web Client supports monitoring of H.263 4CIF information. The H.245 or SDP tab includes the additional information.

The creation of a new H.263 4CIF slide is supported in the IVR Service in addition to the current H.263 IVR slide. If users utilize the default Polycom slides that are delivered with the Collaboration Server, the slide's resolution will be as defined in the profile, i.e. SD, HD, CIF, etc.

For more information see The Resolution Configuration Dialog Box in MPMx/MPMRx Card Configuration Modes

H.263 4CIF Guidelines

- H.263 4CIF is supported with H.323, and SIP and ISDN connection endpoints.
- H.263 4CIF is supported in CP mode only.
- Click&View is supported in H.263 4CIF.
- AES encryption is supported with H.263 4CIF.
- Recording of H.263 4CIF conferences is supported by the RSS 4000 and other devices.
- All video layouts are supported in H.263 4CIF, except 1x1 layout. In a 1x1 layout, the resolution will be CIF.
- H.239 is supported in H.263 4CIF and is based on the same bandwidth decision matrix as for HD.

The CP Resolution Decision Matrix

All the CP resolution options and settings are based on a decision matrix which matches video resolutions to connection line rates, with the aim of providing the best balance between resource usage and video quality at any given line rate.

The following factors affect the decision matrices:

- The Media card(s) installed in the system affect the number of video resources used for each video resolution and frame rate, the supported video protocols and the maximum resolution that can be used by the Collaboration Server.
- The used video protocol: H.264 base Profile or H.264 High Profile. The H.264 High Profile maintains the Video quality at bit rates that are up to 50% lower than previously required. For example, a 512 kbps call will have the video quality of a 1Mbps HD call while a 1Mbps HD call has higher video quality at the same (1Mbps) bit rate.
- A different decision matrix is used for Motion and Sharpness as the quality requirements are different.

The system is shipped with three pre-defined settings of the decision matrix for H.264 Base Profile and three pre-defined settings of the decision matrix for H.264 High Profile with Motion and Sharpness video quality for each of the following resource management schemes:

- · Resource-Quality Balanced (default)
 - A balance between video quality and resource usage. This is the only available resolution configuration in version 6.0.x and earlier.
- Resource Optimized
 - System resource usage is optimized by allowing high resolution connections only at high line rates and may result in lower video resolutions (in comparison to other resolution configurations) for some line rates. This option allows to save MCU resources and increase the number of participant connections.
- Video Quality Optimized
 - Video is optimized through higher resolution connections at lower line rates increasing the resource usage at lower line rates. This may decrease the number of participant connections.

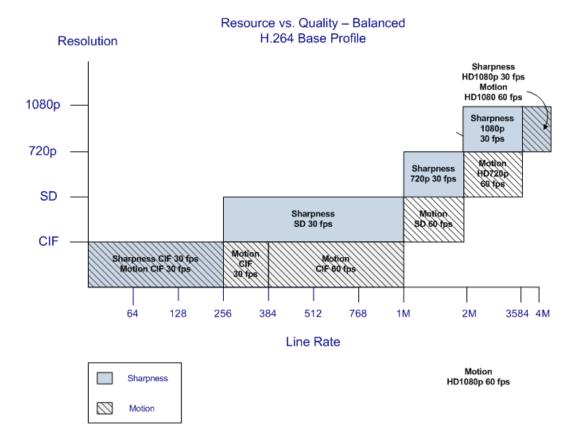
Video Resource Usage

Video resource usage is dependent on the participant's line rate, resolution and Video Quality settings.

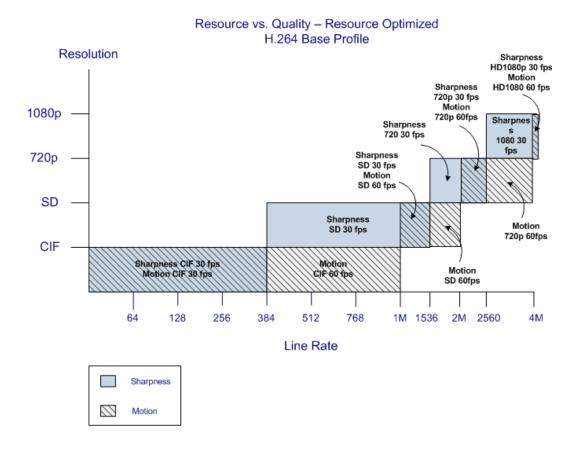
H.264 Base Profile Decision Matrix

The following illustrations show the resolutions used for the various Line Rates for each of the pre-defined optimization settings for H.264 Base Profile and Video Quality setting **Sharpness** and **Motion** for MPMx/MPMRx Card Configuration Modes.

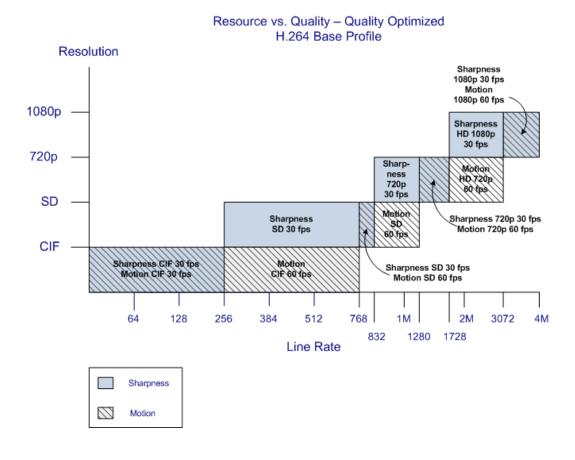
Resolutions used per Line Rates When Resolution Configuration is set to Resource-Quality Balanced Configuration in Sharpness and Motion Mode, MPMx/MPMRx



Resolutions used per Line Rates When Resolution Configuration is set to Resource Optimized Configuration in Sharpness and Motion Mode, MPMx/MPMRx



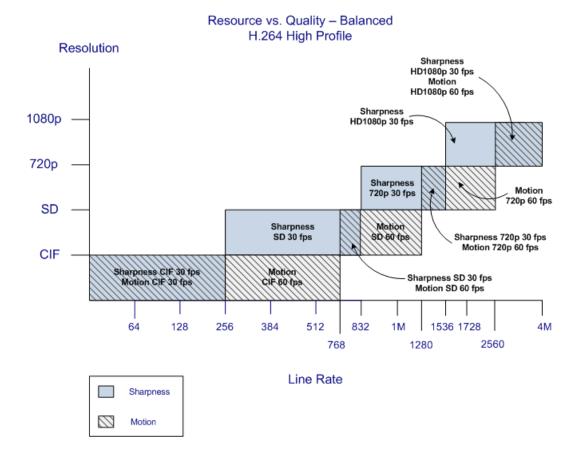
Resolutions used per Line Rates When Resolution Configuration is set to Quality Optimized Configuration in Sharpness and Motion Mode, MPMx



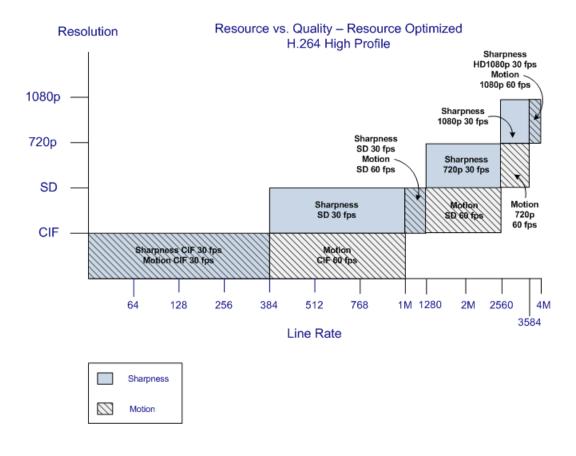
H.264 High Profile Decision Matrices (MPMx/MPMRx)

The following illustrations show the resolutions used for the various Line Rates for each of the pre-defined optimization settings for H.264 High Profile and Video Quality setting **Sharpness** and **Motion** for MPMx/MPMRx Card Configuration Modes.

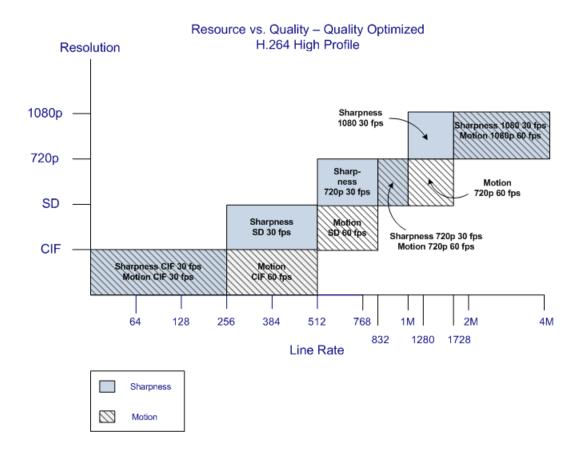
Resolutions used per Line Rates When Resolution Configuration is set to Resource-Quality Balanced Configuration in Sharpness and Motion Mode, MPMx/MPMRx



Resolutions used per Line Rates When Resolution Configuration is set to Quality Optimized Configuration in Sharpness and Motion Mode, MPMx



Resolutions used per Line Rates When Resolution Configuration is set to Resource Optimized Configuration in Sharpness and Motion Mode, MPMx/MPMRx



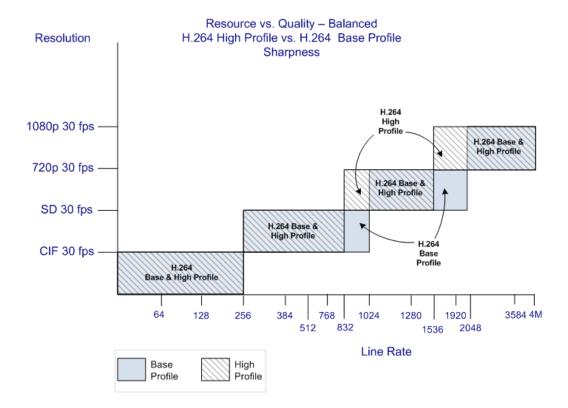
H.264 Base Profile and High Profile Comparison

The following illustrations show a comparison between the resolutions used at various line rates for H.264 baseline and the H.264 High Profile, for Motion and Sharpness Video Quality setting according to the Resolution Configuration Mode (**Balanced**, **Resource Optimized** or **Video Quality Optimized**).

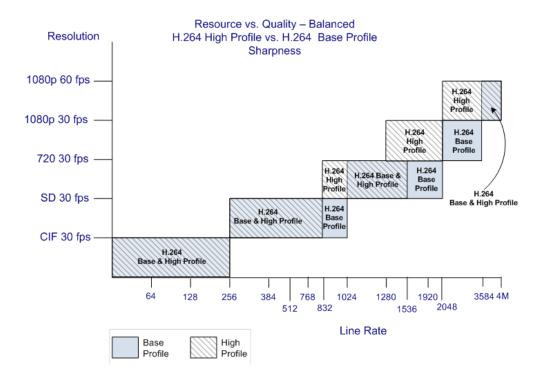
H.264 Base Profile and High Profile Comparison - Sharpness

A comparison between the resolutions used at various line rates for H.264 Baseline and the H.264 High Profile for Sharpness Video Quality setting according to the following Resolution Configuration Modes.

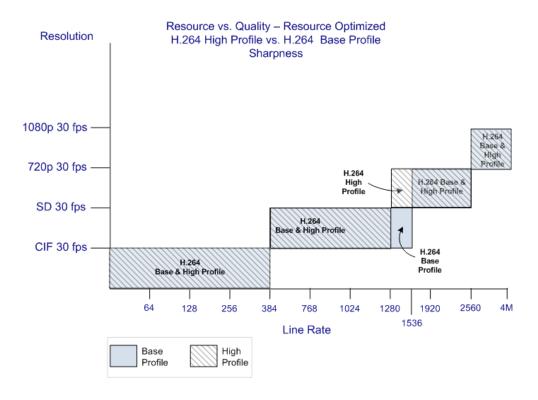
Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Resource-Quality Balanced, MPMx



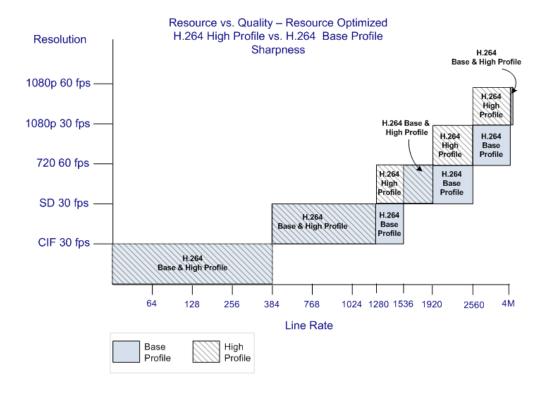
Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Resource-Quality Balanced, MPMRx



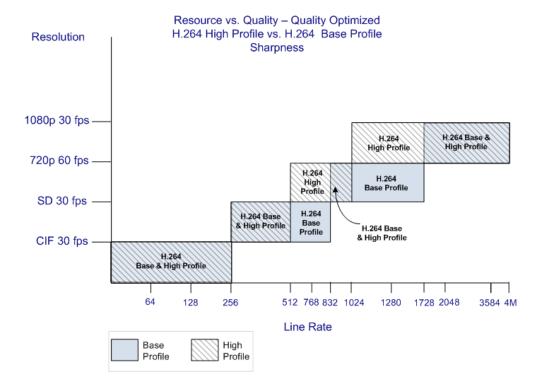
Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Resource Optimized, MPMx



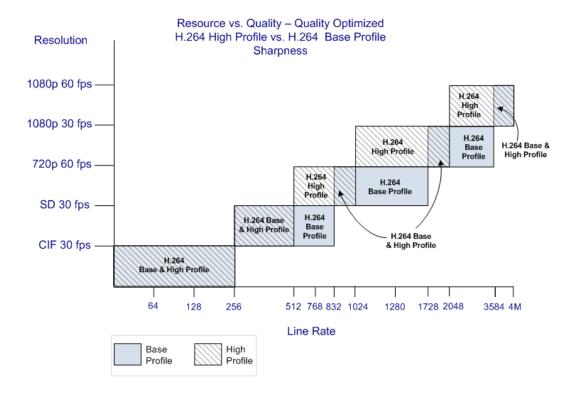
Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Resource Optimized, MPMRx



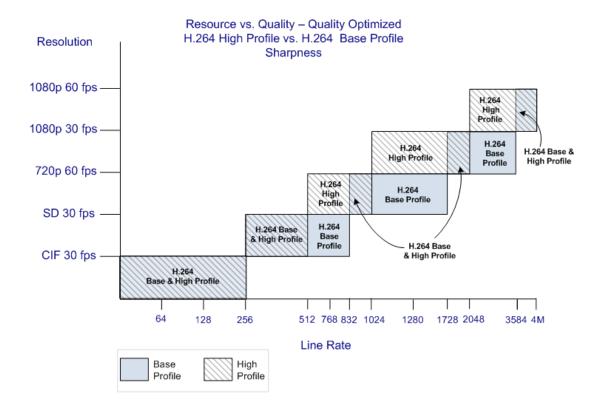
Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Video Quality Optimized, MPMx



Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Video Quality Optimized, MPMRx



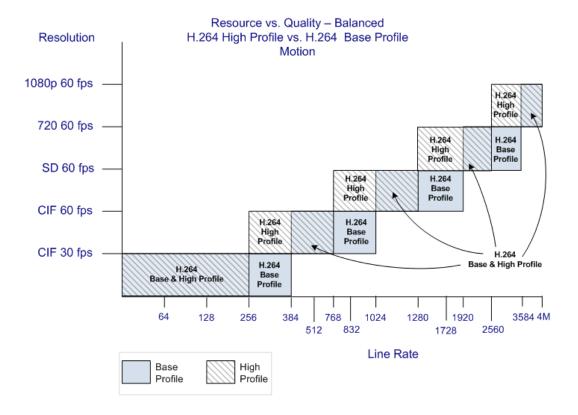
Resolution usage for H.264 High Profile and H.264 Base Profile for Sharpness at various line rates when Resolution Configuration is set to Video Quality Optimized



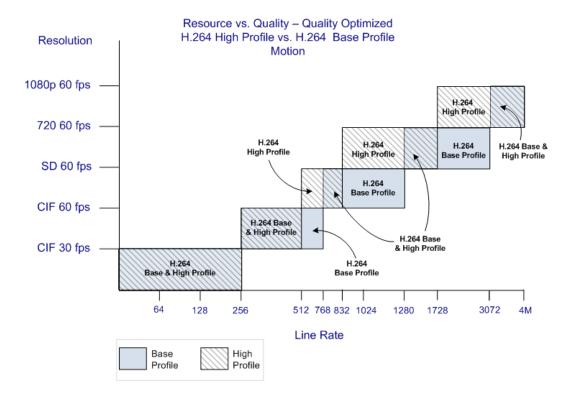
H.264 Base Profile and High Profile Comparison - Motion

A comparison between the resolutions used at various line rates for H.264 Baseline and the H.264 High Profile for Motion Video Quality setting according to the following Resolution Configuration Modes.

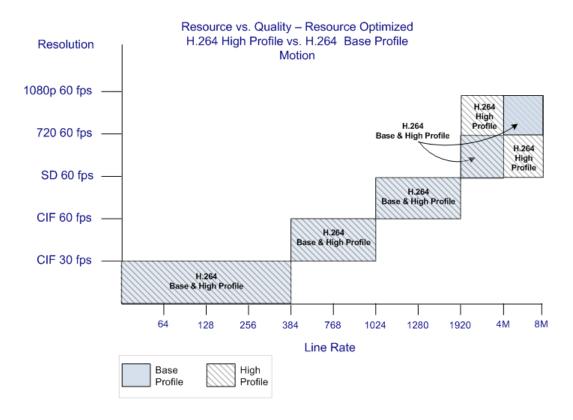
Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource-Quality Balanced



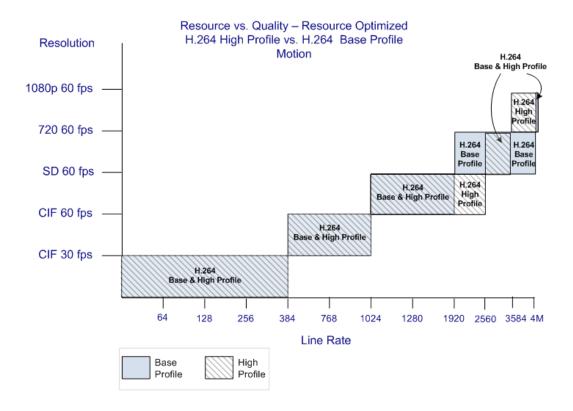
Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Video Quality Optimized



Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource Optimized



Resolution usage for H.264 High Profile and H.264 Base Profile for Motion at various line rates when Resolution Configuration is set to Resource Optimized



Default Minimum Threshold Line Rates and Resource Usage Summary

The following Table summarizes the Default Minimum Threshold Line Rates and Video Resource usage for each of the pre-defined optimization settings for each Resolution, H.264 Profile, Video Quality setting (**Sharpness** and **Motion**) for MPMx/MPMRx Card Configuration Modes.

Default Minimum Threshold Line Rates and Video Resource Usage

			Optimization Mode							
Resolution		Profile	Baland	ced	Resou	rce	Video Quality			
			Sharpness	Motion	Sharpness	Motion	Sharpness	Motion		
De:	Default	High	2048*	1728	2560*	2560	2048*	1472		
HD1080p60	kbps	Base	3584*	3072	4096*	4096	3584*	1728		
HD1080n30	Default	High	1536		4096		1024			
	kbps	Base	4096		4096		1728			

Default Minimum Threshold Line Rates and Video Resource Usage

				Optimization Mode								
Resolution	Resolution		Baland	ced	Resou	rce	Video Quality					
			Sharpness	Motion	Sharpness	Motion	Sharpness	Motion				
HD720p60	Default	High		1280		1920		832				
пьтгорос	kbps	Base		1920		1920		1280				
HD720p30	Default	High	832		1920		512					
пь/20рзо	kbps	Base	1024		1920		832					
SD 60	Default	High		768		1024		512				
3D 60	kbps	Base		1024		1024		768				
SD 30	Default	High	256		384		256					
3D 30	kbps	Base	256		384		256					
CIF 60	Default	High		256		384		256				
OIF OU	kbps	Base		384		384		256				
CIF 30	Default	High	64	64	64	64	64	64				
OIF 30	kbps	Base	64	64	64	64	64	64				



- * Applicable to Collaboration Server (RMX) 1800 and MPMRx only
- The table above lists resource consumption for H.264.
- For H.263 with MPMx cards:
 - ▲ CIF resolution consumes 1.5 resources.
 - ▲ 4CIF resolution consumes 3 resources.

Resolution Configuration for CP Conferences

The **Resolution Configuration** dialog box enables you to override the default video resolution decision matrix, effectively creating your own decision matrix. The minimum threshold line rates at which endpoints are connected at the various video resolutions can be optimized by adjusting the resolution sliders.

System resource usage is also affected by the Resolution Configuration settings.

For more information see Video Resource Usage and Default Minimum Threshold Line Rates and Resource Usage Summary.

Guidelines

 Resolution Slider settings affect all Continuous Presence (CP) conferences running on the Collaboration Server. Video Switched conferences are not affected.



On the RealPresence Collaboration Server (RMX) 1500 MPMx-Q assembly, the use of HD with Continuous Presence requires an additional license. In the Resource Report and Resolution Configuration panes, HD settings are displayed but are not enabled and if HD is selected the system will enable SD by default.

- A system restart is not needed after changing the Resolution Slider settings.
- Resolution Slider settings cannot be changed if there are ongoing conferences running on the Collaboration Server. The displayed sliders and the resolutions change according the Card Configuration Mode: MPMx or MPMRx.

Accessing the Resolution Configuration Dialog Box

The **Resolution Configuration** dialog box is accessed by clicking **Setup > Resolution Configuration** in the Collaboration Server **Setup** menu.

The Resolution Configuration dialog box display changes according to the Card Configuration Mode:

- MPMx
- MPMRx

This chapter describes Resolution Configuration in MPMx Card Configuration Mode.

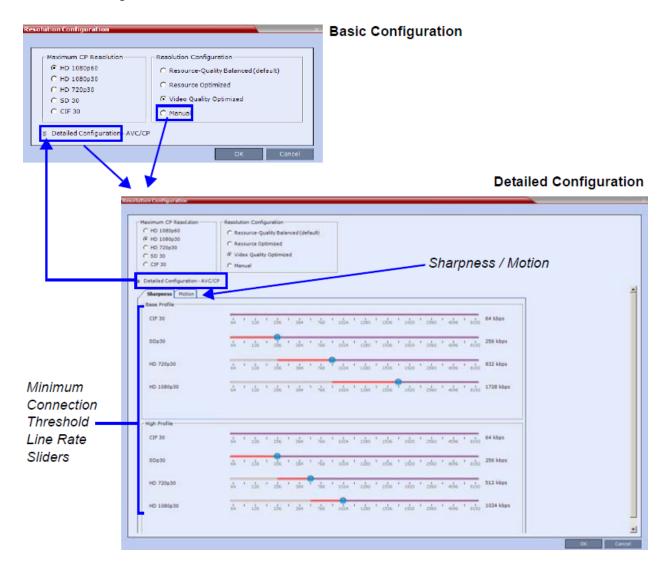
The Resolution Configuration Dialog Box in MPMx/MPMRx Card Configuration Modes

The **Resolution Configuration** - **Basic Configuration** dialog box is the first dialog box displayed when the Collaboration Server is in the MPMx/MPMRx Card Configuration Mode.

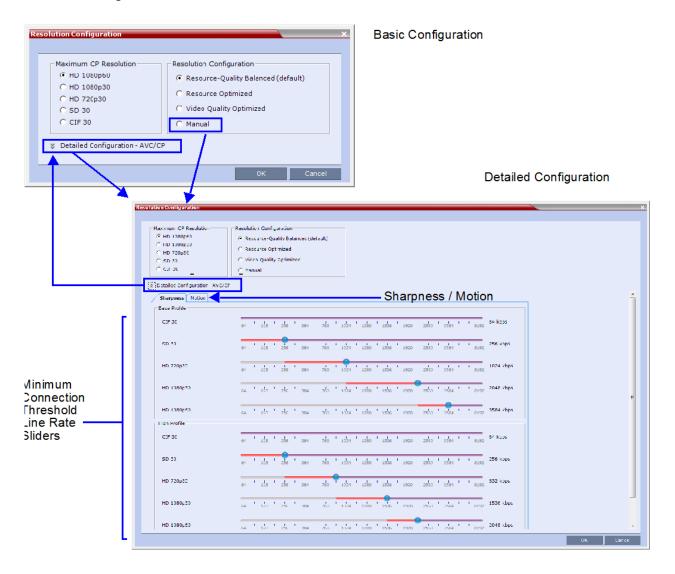
Clicking the **Detailed Configuration** button toggles the display of the **Detailed Configuration** pane, which displays sliders for modifying minimum connection threshold line rates for endpoints that support H.264 Base Profile or High Profile. The **Detailed Configuration** pane can also be opened by clicking the **Manual** radio button in the **Resolution Configuration** pane.

Sharpness and **Motion** settings are accessed by clicking the **Sharpness** and **Motion** tabs when the **Detailed Configuration** is open.

Resolution Configuration - MPMx



Resolution Configuration - MPMRx



Resolution Configuration - Basic

The **Resolution Configuration** basic dialog box contains the following panes:

- Max CP Resolution Pane
- Resolution Configuration Pane



Maximum CP Resolution Pane

In MPMx/MPMRx Card Configuration Mode the Collaboration Server can be set to one of the following **Maximum CP Resolutions**:

- HD 1080p60
- HD 1080p30
- HD 720p30
- SD 30
- CIF 30

Limiting Maximum Resolution

Before a selection is made in this pane, the Maximum CP Resolution of the system is determined by the **MAX_CP_RESOLUTION** System Flag.

The **MAX_CP_RESOLUTION** flag value is applied to the system during First Time Power-on and after a system upgrade.

The default flag value is **HD1080** setting the **Maximum CP Resolution** value in the **Resolution Configuration** dialog box to 1080p60.

All subsequent changes to the Maximum CP Resolution of the system are made by selections in this pane.

The Maximum Resolution can further be limited per conference or per participant endpoint.

The Maximum Conference Resolution, can be limited via the **Profile - Video Quality** dialog box. For more information see Defining New Profiles.

The Maximum Resolution can further be limited per participant endpoint via the **Participant - Properties** dialog box. For more information see Managing the Address Book.

Resolution Configuration Pane

The user can select from 3 pre-defined Resolution Configurations or select a manual Resolution Slider adjustment mode. The pre-defined settings can be accepted without modification or be used as the basis for manual fine tuning of resolution settings by the administrator.

The **Manual** radio button is automatically selected if any changes are made to the Resolution Sliders.

The Resolution Configurations are:

Resource-Quality Balanced (default)

A balance between the optimized video quality and optimized resource usage.



Use this option:

- When the priority is to maintain a balance between resource usage and video quality.
- When it is necessary to maintain backward compatibility with previous versions.
- When working with Polycom DMA/RealPresence Resource Manager.

The **Balanced** settings are described in the section: Default Minimum Threshold Line Rates and Resource Usage Summary.

Resource Optimized

System resource usage is optimized by allowing high resolution connections only at high line rates and may result in lower video resolutions (in comparison to other resolution configurations) for some line rates.



Use this option when the priority is to save MCU resources and increase the number of participant connections.

The **Resource Optimized** settings are described in the section: Default Minimum Threshold Line Rates and Resource Usage Summary.

Video Quality Optimized

Video is optimized through higher resolution connections at lower line rates increasing the resource usage at lower line rates. This may decrease the number of participant connections.



Use this option when the priority is to use higher video resolutions while decreasing the number of participant connections.

The Video Quality Optimized settings are described in the section: Default Minimum Threshold Line Rates and Resource Usage Summary.

Manual

Manually adjusting the sliders to accommodate local conferencing requirements.

Resolution Configuration - Detailed

The **Resolution Configuration -Detailed** dialog box contains the following panes:

- Sharpness Resolution sliders
- Motion Resolution sliders

Sharpness and Motion

Sharpness and Motion are Video Quality settings that are selected per conference and are defined in the conference Profile. A conference with Sharpness selected in its Profile uses the Sharpness settings of the Resolution Configuration and a conference with Motion selected in its Profile uses the Motion settings of the Resolution Configuration dialog box.

The **Sharpness** and **Motion** tabs in the **Resolution Configuration** dialog box allow you to view and modify **Resolution Configuration** settings for conferences with either Video Quality setting.

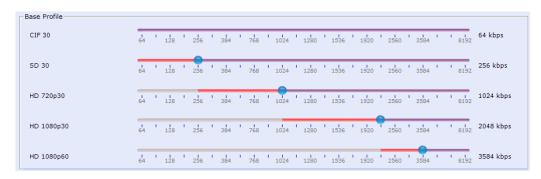
The **Sharpness** and **Motion** tabs include separate settings for Base Profile and High Profile as the Collaboration Server uses two decision matrices (Base Profile, High Profile) to enable endpoints to connect according to their capabilities.

H.264 High Profile allows higher quality video to be transmitted at lower bit rates. However, setting minimum bit rate thresholds that are lower than the default may affect the video quality of endpoints that do not support the H.264 High Profile.

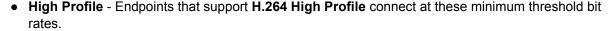
Resolution Configuration Sliders

The **Detailed Configuration** dialog box allows you to configure minimum connection threshold bit rates for endpoints that support H.264 High Profile and those that do not support H.264 High Profile by using the following slider panes:

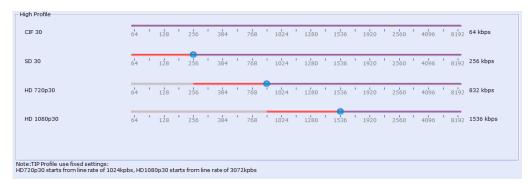
• Base Profile - Endpoints that do not support H.264 High Profile connect at these minimum threshold bit rates.











Although the default minimum threshold bit rates provide acceptable video quality, the use of higher bit rates usually results in better video quality but will require more resources.

The Base Profile and High Profile sliders operate in the same manner in Sharpness and in Motion.

Video Resource usage is affected by the Resolution Configuration settings. The lower the line rate threshold set for a certain resolution the more resources will be used to connect that participant (as a higher resolution will be used).

Modifying the Resolution Configuration in MPMx Card Configuration Mode

Moving the slider of a certain resolution to the left reduces the line rate threshold required for the endpoints to connect using that resolution (resulting in higher video quality, more video resources). Moving the slider to the right, increases the line rate required for the endpoint to connect using that resolution (resulting in lower video quality, less video resources).



The following example demonstrate the usage of the sliders.



- Moving the HD720p30 resolution slider from 1024kbps to 1920kbps increases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 1024kbps and 1920kbps that would have connected at HD 720p30 resolution will instead connect at SD 30 resolution. Each of the affected endpoints will connect at lower resolution but will use less video resources.
- Moving the HD1080p30 resolution slider from 4096kbps to 2560kbps decreases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 2560kbps and 4096kbps that would have connected at HD 720p30 resolution will instead connect at HD 1080p30 resolution. Each of the affected endpoints will connect at higher resolution but will use more video resources.
- Moving the HD1080p60 resolution slider from 3584kbps to 2560kbps decreases the minimum connection threshold line rate for that resolution. Endpoints connecting at line rates between 2560kbps and 4096kbps that would have connected at HD 1080p30 resolution will instead connect at HD 1080p60 resolution. Each of the affected endpoints will connect at higher resolution but will use more video resources.

Flag Settings

Setting the Maximum CP Resolution for Conferencing

The **MAX_CP_RESOLUTION** flag value is applied to the system during First-time Power-up and after a system upgrade. The default value is **HD1080**.

All subsequent changes to the Maximum CP Resolution of the system are made by selections in the **Max CP Resolution** pane of the **Resolution Configuration** dialog box.

The Maximum CP Resolution of the Collaboration Server can be set to one of the following resolutions:

- HD 1080p60
- HD 1080p30
- HD 720p30
- SD 30
- CIF 30

Minimum Frame Rate Threshold for SD Resolution

The **MINIMUM_FRAME_RATE_THRESHOLD_FOR_SD** System Flag can be added and set to prevent low quality, low frame rate video from being sent to endpoints by ensuring that an SD channel is not opened at frame rates below the specified value. For more information see Modifying System Flags.

Limiting The Maximum Negotiated Bit Rate for SD and Lower Resolutions

For systems containing MPM Rx cards, the **LIMIT_SD_AND_CIF_BW_MPMRX** System Flag, when added to **system.cfg** and set to **YES** (default), limits the maximum negotiated and opened bit rate for resolutions equal or lower than SD to 1Mbps. When set to **NO** no limitation is applicable to SD and CIF bit rates.

Additional Video Resolutions in MPMx Card Configuration Mode

The following higher video quality resolutions are available with when the Collaboration Server is working in MPMx Mode:

• CIF	352 x 288 pixels	at 50 fps.
• WCIF	512 x 288 pixels	at 50 fps
• WSD	848 x 480 pixels	at 50 fps
• W4CIF	1024 x 576 pixels	at 30 fps
• HD 720p	1280 x 720 pixels	at 60 fps (symmetric with MPMx)
• HD 1080p	1920 x 1080 pixels	at 30 fps (symmetric with MPMx)
• HD 1080p	1920 x 1080 pixels	at 60 fps (asymmetric with MPMx)



The video resolution transmitted to any endpoint is determined by the endpoint's capabilities, the conference line rate, the Conference Profile's Motion and Sharpness settings and the Collaboration Server's Card Configuration Mode (MPMx or MPMRx).

w448p Resolution

For improved interoperability with Tandberg MXP 990/3000 endpoints, the appropriate System Flag settings will force the Collaboration Server to send w448p (768x448 pixels) at 25fps as a replacement resolution for WSD15 (848x480) and SD15 (720x576 pixels).

Guidelines

- The w448p resolution is supported:
 - > In CP mode.
 - ➤ At conference line rates of 384kbps and 512kbps.
 - With H.323, SIP, and ISDN endpoints.
 H.323 endpoints must identify themselves as Tandberg MXP during capabilities exchange.
 - In all Video Layouts.
 - ➤ In 1x1 Layout:
 - When Video Clarity is Off, the Collaboration Server transmits the same resolution as it receives.
 - ♦ When Video Clarity is **On**, the Collaboration Server changes the transmitted resolution to w448p.

For more information see Video Clarity™.

• Resource consumption for the w448p resolution is the same as for SD and WSD resolutions.

The following table lists the video outputs from the Collaboration Server to the Tandberg Endpoints for both 16:9 Aspect Ratio when the w448p resolution is enabled.

Video Output to Tandberg Endpoints- Aspect Ratio 16:9

	Video Quali	ty	- Line	Resolution	Frame Rate fps	Resolutio n	Frame Rate fps
Network Environment	Tandberg	Collaboration Server	Rate Kbps	Tandberg to Collaboration	dberg to laboration Server		on Server g
H.323	Motion	Sharpness	384	512x288	30	768x448	25
SIP			512	768x448	30	768x448	25
H.323	Sharpness *	Sharpness	384	1024x576	15	768x448	25
SIP	•		512	1024x576	15	768x448	25

^{*} It is recommend to set the endpoint to **Motion** to ensure the transmission of the higher frame rates of 25fps/30fps to the Collaboration Server.

The following table list the video outputs from the Collaboration Server to the Tandberg Endpoints for 4:3 Aspect Ratio when the w448p resolution is enabled.

Video Output to Tandberg Endpoints - Aspect Ratio 4:3

Video Quality		_ Line	Resolution	Frame Rate fps	Resolution	Frame Rate fps	
Network Environment	Tandberg	Collaboration Server	Rate Kbps	Tandberg to Collaboration Server		Collaboration to Tandberg	n Server
H.323	Motion	Sharpness	384	576x448 ‡	25	768x448	25
SIP ISDN			512	576x448 ‡	25	768x448	25
H.323	Sharpness*	Sharpness	384	4CIF	15	768x448	25
SIP ISDN			512	4CIF	15	768x448	25

^{*} It is recommend to set the endpoint to **Motion** to ensure the transmission of the higher frame rates of 25fps/30fps to the Collaboration Server.

‡ *MXP* 990/3000 endpoints transmit 576x448 pixels. Other MXP endpoints may transmit other resolutions eq. CIF.

Content

Sharing and receiving Content is supported.

Bandwidth allocated to the Content channel during Content sharing may cause the video resolution to be decreased as from w448p to w288p.

When Content sharing stops and the full bandwidth becomes available, video resumes at the previous w448p resolution.

For more information see the Video Preview (AVC Participants Only).

Packet Loss Compensation

If there is Packet Loss in the network and Dynamic Bandwidth Allocation (DBA) is activated, allocating bandwidth for Lost Packet Recovery, video resolution decreases from w448p to w288p.

When Packet Loss ceases and DBA no longer needs to allocate bandwidth for Lost Packet Recovery, the full bandwidth becomes available and video resumes at the previous w448p resolution.

For more information see the Packet Loss Compensation (LPR and DBA) AVC CP Conferences.

Enabling Support of the w448p Resolution

w448p resolution support for Tandberg endpoints requires setting of the following entities:

- · Tandberg endpoint
- Collaboration Server flags
- Collaboration Server Conference Profile

Collaboration Server System Flag Settings

On the Collaboration Server, the **Video Quality** field in the **New Profile - Video Quality** dialog box must be set to **Sharpness**.

For more information see Defining New Profiles.

Additional Intermediate Video Resolutions

Two higher quality, intermediate video resolutions replace the transmission of CIF (352 x 288 pixels) or SIF (352 x 240 pixels) resolutions to endpoints that have capabilities between:

- CIF (352 x 288 pixels) and 4CIF (704 x 576 pixels) the resolution transmitted to these endpoints is 432 x 336 pixels.
- SIF (352 x 240 pixels) and 4SIF (704 x 480 pixels) the resolution transmitted to these endpoints is 480 x 352 pixels.

The frame rates (depending on the endpoint's capability) for both intermediate resolutions are 25 or 30 fps.

Sharing Content During Conferences

Content such as graphics, presentations, documents or live video can be shared with conference participants using the H.239 (H.323) or BFCP (SIP) protocol, which are the standard protocols for content sharing or Polycom's proprietary protocol People+Content.

Content Sharing Using H.239 Protocol

The H.239 protocol allows compliant endpoints to transmit and receive two simultaneous video streams:

- **People video stream** displays the video of the people participating in the meeting. This is the primary video channel of the conference and it is displayed in all the conferencing modes.
- **Content video stream** displays the content being shared, such as graphic presentations, files, movies, or any information that can be displayed on the computer's screen.

By default, all conferences, Entry Queues, and Meeting Rooms launched on the Collaboration Server have H.239 content sharing capabilities.

Endpoints may not send Content while connecting to an Entry Queue.

Endpoints without H.239 capability can connect to the video conference without Content.

Cascade links declare H.239 capabilities and they are supported in Star and MIH cascading topologies. For more details, see Cascading Conferences - H.239-enabled MIH Topology.

Content Sharing Using People+Content Protocol

People+Content utilizes a different signaling protocol and is Polycom's proprietary equivalent of H.239. It is supported in CP conferences.

Guidelines for Content Sharing Using People+Content Protocol

- All network environments are supported.
- Conferences can include a mix of endpoints that support H.239 or People+Content.
- All endpoints will receive Content at the highest resolution common to all connected endpoints.
- H.239 is supported in MIH, Star and Basic Cascading topologies.
- People+Content is supported in cascaded conferences but cannot be used as the protocol for a cascade link.
- If an endpoint supports both H.239 and People+Content protocols, H.239 is selected as the preferred communications protocol.
- H.263 Annex T and H.264 protocols are supported for Content transmission.

- People+Content is enabled by default. It can be disabled for all conferences and endpoints by
 manually adding the ENABLE_EPC System Flag to the System Configuration and setting its value
 to NO (default setting is YES).
- Endpoints that support People+Content (for example, FX endpoints) may require a different signaling
 protocol. For these endpoints, manually add the System Flag CS_ENABLE_EPC to the System
 Configuration and set its value to YES (default value is NO).
- Content sharing is not supported in Microsoft ICE environment (BFCP protocol).
- Video endpoints that do not support SIP Content (such as PVX), can receive Content on the People channel if the conference is set to **Send Content to Legacy Endpoints**. For more details see, Sending Content to Legacy Endpoints (AVC Only).
- HD1080p30 Content is supported:
 - On RealPresence Collaboration Server model 1800.
 - On RealPresence Collaboration Server models 2000 and 4000, with MPMRx cards installed.
 - > At a maximum content rate of 2048 kbps on RealPresence Collaboration Server 2000 and 4000.
 - > At a maximum content rate of 4096 kbps on RealPresence Collaboration Server 1800.
- HD1080p60 Content is supported:
 - On the RealPresence Collaboration Server 1800.
 - In the normal (switched) Content mode.
 - In AVC-CP conferencing mode only.
 - With SIP and H.323 endpoints
 - ➤ With the H.263 and H.264 Auto Selection, H.264 HD and H.264 Cascade and SVC Optimized. Content protocol options.
 - With Customized Content Rates.
 - In (H.323) Cascaded conferences.
 - On Legacy Endpoints when the Send Content to Legacy Endpoints option is selected.
 - Content is shared using the video channel.
- HD1080p30 and HD1080p60 Content are not supported:
 - By MCUs containing MPMx cards.
 - ➤ With RealPresence® Content Sharing Suite for Microsoft® Lync® endpoints.
 - > By ISDN endpoints.
 - ➤ When TIP compatibility is set to **Prefer TIP** or **Video and Content**.
 - TIP Content is shared at XGA Resolution at 5 frames per second.
 - By H.263 Content Protocol.
 - ➤ In Multiple Content Resolutions mode.
 - ▶ If the Content was defined as High Profile, endpoints which support only Base Profile Content will not be able to receive Content using the Content channel. If the Send Content to Legacy Endpoints option is selected they can receive Content shared using the video channel.

- In non-Cascaded environments:
 - Content Video Switching mode, Content sharing rate, resolution and frame rate is negotiated according to the capabilities of highest common capabilities of all endpoints connected to the conference.
 - Endpoints which do not support High Profile will not receive content through the Content channel.
- In Cascaded environments:
 - Content sharing rate, resolution and frame rate must be pre-defined and endpoints which do not support these capabilities will not receive content though the Content channel.
 - For more information see Sharing Content Using Multiple Content Resolutions Mode.

SIP BFCP Content Capabilities

SIP Clients supporting BFCP over UDP, when connected to conferences on the Collaboration Server, can share Content with endpoints supporting the following Content sharing protocols:

- BFCP/TCP
- BFCP/UDP
- H.323/ H.239
- H.323 /Polycom People+Content
- ISDN Content (Collaboration Server 1500/2000/4000)

Guidelines for Using SIP BFCP Content

For SIP Clients that support both BFCP/TCP and BFCP/UDP:

- The preferred protocol is BFCP/UDP.
- When used in Cascading conferences, the Cascade Link must be H.323.
- BFCP/UDP is supported in both IPv4 and IPv6 addressing modes.
- BFCP utilizes an unsecured channel (port 60002/TCP) even when SIP TLS is enabled. If security is
 of higher priority than SIP content sharing, SIP People+Content can be disabled. To do this manually
 add the ENABLE_SIP_PEOPLE_PLUS_CONTENT System Flag to the System Configuration and
 set its value to NO.
- SIP People+Content and BFCP capabilities are by default declared to all endpoints. If, however, the
 endpoint identity is hidden by a proxy server, these capabilities will not be declared by the
 Collaboration Server. Capabilities declaration is controlled by the
 ENABLE_SIP_PPC_FOR_ALL_USER_AGENT system flag.
 - The default value of the **ENABLE_SIP_PPC_FOR_ALL_USER_AGENT** system flag is **YES** resulting in BFCP capability being declared with all vendors' endpoints unless it is set to **NO**. When set to NO, the Collaboration Server will declare SIP People+Content and BFCP capabilities to Polycom and Avaya endpoints.
- The ENABLE_FLOW_CONTROL_REINVITE System Flag should be set to NO when SIP BFCP is enabled.
- If these System Flags don't exist in the system, they must be manually added. For more information see Modifying System Flags.
- BFCP capabilities are not supported in Microsoft ICE environment.
- BFCP over TCP is not supported in Ultra Secure Mode (Collaboration Server 1500/2000/4000).

BFCP support in dial-out Connections

For dial-out connections to SIP Clients, BFCP/UDP protocol can be given priority by adding the adding the SIP BFCP DIAL OUT MODE system flag to system.cfg and setting its value to UDP.

The Collaboration Server's Content sharing determined by the System Flag's settings and SIP Client capabilities are summarized in the following table.

System Flag - SIP_BFCP_DIAL_OUT_MODE

Flag Value	SIP Client: BFCP Support						
riag value	UDP	TCP	UDP and TCP				
AUTO (Default)	BFCP/UDP selected as Content sharing protocol.	BFCP/TCP selected as Content sharing protocol.	BFCP/UDP selected as Content sharing protocol.				
UDP		Cannot share Content.					
TCP	Cannot share Content.	BFCP/TCP selected as Content sharing protocol.					

For more information see Manually Adding and Deleting System Flags.

BFCP support in dial-in Connections

- The Collaboration Server will share content with dial-in SIP clients according to their preferred BFCP protocol.
- SIP clients connected as audio only cannot share content.

Video Transmission Methods for Sharing Content

Content can be shared using the following video transmission methods:

- Content Highest common parameters (also known as Content Video Switching)
- Multiple Content Resolutions (CP Conferencing Mode only)

In Content Video Switching mode - The content is negotiated to highest common capabilities supported by the endpoints connected to the conference. If the conference includes participants that support lower content capabilities (such as H.263) and higher content capabilities (H.264), content will be sent at the lower capabilities supported by all endpoints, resulting in lower content quality seen by all endpoints.

In this mode, the content is set according to the capabilities of all the participants currently connected to the conference. If all the connected participant support the H.264 protocol, the Content will be started with H.264 capabilities. If then an endpoint supporting only H.263 protocol connects, the content is stopped in order to switch to H.263 and has to be resent. If the H.263 participant leaves the conference and only H.264 capable endpoints remain connected, content is stopped in order to switch back to H.264 and has to be resent.

In Multiple Content Resolutions mode - The content is shared in multiple streams, one for each video protocol: H.263 and H.264. A separate video resource is used to process the Content shared with H.264-capable endpoints and another for content shared with H.263-capable endpoints, with each endpoint receiving its highest possible quality. This allows endpoints with different protocols to connect and disconnect without having to restart Content sharing in the middle of a conference.

In this mode, endpoints that do not support the content capabilities set for the conference will receive the content over the video (people) channel (Legacy content).

Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode

This section describes the possible content sharing parameters when content Highest Common mode is used:

- Content Settings
- Content Protocol
- Content Resolution

Content Settings

The Content channel can transmit one of the following modes:

- **Graphics** for standard graphics. This is the default mode in AVC conferences and the only supported mode for SVC conferences.
- Hi-res Graphics (AVC CP Only) requiring a higher bit rate, for high quality display or highly detailed graphics.
- Live Video (AVC CP Only) highest bit rate, for video clips or live video display.
- Customized Content Rate (AVC CP Only) that allows manual definition of the Conference Content Rate.

AVC CP Content Setting

For Graphics, Hi-res Graphics and Live Video, the highest common Content bit rate is calculated for the conference each time an endpoint connects. Therefore, if an endpoint connects to an ongoing conference at a lower bit rate than the current bit rate, the Content bit rate for the current conference is re-calculated and decreased.

Bit rate allocation by the MCU is dynamic during the conference and when the Content channel closes, the video bit rate of the People conference is restored to its maximum.

During a conference the MCU will not permit an endpoint to increase its bit rate, it can however change its Content resolution. The Collaboration Server can decrease the allocated Content bit rate during a conference.

The following tables summarizes the bit rate allocated to the Content channel from the video channel in each of the Content Settings according to the conference line rate for Base Profile and High Profile settings.

For more information see H.264 Base Profile and High Profile Comparison.

Highest Common Content Bit Rate Allocation for Base Profile

	Cont	tent Bit	Rate	Allocat	ion pe	r Confe	erence L	ine Rate	(Kbps)						
Content	64	128	256	384	512	768	1024	1152	1536	1920	2048	2560	3072	4096	6144
Settings	96	192	320			832		1280	1728				3584		
								1472							
Graphics 3	3%														
Common < 1080p15	0	64	64	128	128	256	256	384	512	512	512	768	768	1280	1280
< 1080p30															2048
Hi-res Grap	hics 5	0%													
Common < 1080p15	0	64	128	192	256	384	512	512	768	768	1024	1280	1536	15	36
< 1080p30]													00.40	2048
< 1080p60														2048	3072
Live Video	66%														
Common < 1080p15	0	64	128	256	384	512	512	768	1024	1280	1280	1536		1536	
1080p30]												00.40	00.40*	2048
1080p60	1												2048	2048*	4096

^{* 2560 (}RealPresence Collaboration Server 1800)

The table above applies to single MCU (non-cascading) and non-SVC enabled conferences.

Conference Line Rate and Content Allocation Rate for Base Profile

Bit Rate Allocated to Content	Content					
Channel (Kbps)	Maximum Resolution	Frames/Second				
64-512	H.264 HD720	5				
512-768	H.264 HD720	30				
768-1536	H.264 HD1080	15				
1536-2048 / 3072 (RealPresence Collaboration Server 1800)	H.264 HD1080	30				
3072-4096	H.264 HD1080	60				

Highest Common Content Bit Rate Allocation for High Profile

	Cont	ent Bit	Rate A	llocati	ion per	Confe	rence L	ine Rate	(Kbps)												
Content	64	128	256	384	512	768	1024	1152	1536	1728	1920	2560	3072	4096	6144						
Settings	96	192	320			832		1280			2048		3584								
								1472													
Graphics 3	3%																				
Common					.000000000			0000000000		000000000000000000000000000000000000000		000000000000000000000000000000000000000		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		000000000000000000000000000000000000000	1280				
< 1080p30	0	64	64	128	128	256	256	384	512	512	512	768	768	1280	20.40						
< 1080p60																					2048
Hi-res Grap	hics 50	0%																			
Common < 1080p15													1280	1280	1280						
<1080p30	0	0 64 12	128	128 256	384	512	512	768	768 1024	1280	1024	1280	4500	00.40	2048						
<1080p60]												1536	2048	3072						
Live Video	66%																				
Common < 1080p15		, normannan	, and a second second									1280	1280	1280	1280						
<1080p30	0	64	128	256	384	512	512	768	1024	1280	1280	4500	20.40	2048	2048						
<1080p60]											1536	2048	2560	4096						

The table above applies to single MCU (non-cascading) and non-SVC enabled conferences.

Conference Line Rate and Content Allocation Rate for High Profile

Bit Rate Allocated to Content	Content					
Channel (Kbps)	Maximum Resolution	Frames/Second				
64-384	H.264 HD720	5				
384-512	H.264 HD720	30				
512-768	H.264 HD1080	15				
768-2048	H.264 HD1080	30				
2048-4096	H.264 HD1080	60				

SVC Only and Mixed CP and SVC Content Setting

The Content channel is transmitted in **Graphics** mode only.

Content Protocols

Two Content Protocols can be used for sharing content:

- H.263 (CP and mixed CP and SVC)
- H.264 (all conferencing modes)

H.264 offers higher quality content, but is not supported by legacy endpoints. Depending on the endpoints capabilities, you can determine the content sharing experience by selecting the appropriate protocol and system behavior from the Content Protocol list:

- H.263 & H.264 Auto Selection (AVC CP Only)
- **H.263** (AVC CP Only)
- **H.264 HD** (AVC CP Only)
- H.264 Cascade and SVC Optimized (all conferences)

H.263 & H.264 Auto Selection (AVC CP Conferences)

This option should be selected when Content is to be shared using a mix of H.263-supporting and H.264-supporting endpoints. (In versions up to and including 7.6, this is named Up to H.264.)

Bit rate allocation to the Content channel by the Collaboration Server is dynamic according to the conference line rate and Content Setting selected for the conference.

If an endpoint that supports only H.263 for Content Sharing connects to a conference with Content Protocol set to H.263 & H.264 Auto Selection:

- Content is shared using H.263 even if H.264-supporting endpoints are connected.
- Content is shared using H.264 if all connected endpoints have H.264 capability.
- If the first endpoint to connect to the conference only supports H.263, the H.263 protocol is used for Content for all conference participants.
- If Content is already being shared using the H.264 protocol when a H.263 endpoint connects, Content sharing is stopped and must be manually restarted using H.263 (i.e. the endpoint using H.263 Content Protocol must connect first), for all participants to receive content. If the H.263 endpoint disconnects, Content sharing must be manually stopped and restarted and will automatically upgrade to the H.264 protocol.
- Endpoints that do not have at least H.263 capability can connect to the conference but cannot share Content.
- This option is not available in SVC Conferencing Mode and CP and SVC Conferencing Mode (applicable to AVC endpoints only).

H.263 (AVC CP Conferences)

Select this option when most of the endpoints support H.263 and some endpoints support H.264. In such a case, all endpoints will share content using the H.263 protocol, and this protocol will not change throughout the conference (fixed mode).

Bit rate allocation to the Content channel by the Collaboration Server is dynamic according to the conference line rate and Content Settings selected for the conference. For more information see Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode.

This option is not available in SVC Conferencing Mode and CP and SVC Conferencing Mode.

H.264 HD (AVC CP default)

The **H.264 HD** option should be selected only if most endpoints in the conference support H.264 to ensure high quality Content.

When this protocol option is selected, endpoints must connect at Content bit rates above a minimum as specified by specific System Flags to ensure high quality Content for all participants. For more information about System Flags see Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD.

Bit rate allocation to the Content channel by the Collaboration Server is dynamic according to the conference line rate and Content Setting selected for the conference. For more information see Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode.

Endpoints that do not support H.264, or those that do not meet the minimum line rate threshold for the Content Setting along with ISDN endpoints, are connected as Legacy Endpoints and receive content through their video channel will not receive content. If the Send Content to Legacy Endpoints selection is disabled, these endpoints will not receive content.

Guidelines for Sharing Content Using H.264 HD

- Only endpoints that support H.264 capability at a resolutions of HD720p5 or higher will be able to receive and send Content.
- This option is not available in SVC Conferencing Mode and CP and SVC Conferencing Mode.
- When H.264 HD is selected, the Send Content to Legacy Endpoints selection is enabled by default in the Conference Profile – Video Settings tab.
- Maximum supported content resolution is HD 720p.
- Once an endpoint is categorized as a Legacy Endpoint and receives the content over the video channel, it remains in this mode without the ability to upgrade to H.264 HD content and receive content over the Content channel.
- The minimum Content Rate required for allowing a participant to share Content is the lower valued
 parameter when comparing the System Flag setting (H.264 HD System Flags) and the content bit
 rate allocation derived from the conference line rate (Participant Content Sharing Based on
 Connection Line Rate and System Flag Setting).

When the flag settings enable an endpoint to share Content at a content rate that is lower than the conference content rate (Participant Content Sharing Based on Connection Line Rate and System Flag Setting), the content rate of the entire conference is reduced to the content rate supported by that endpoint.

Setting the Minimum Content Rate for Each Content Quality Setting for H.264 HD

System Flags determine the minimum line rate required for endpoints to share H.264 high quality content for each Content Setting: Graphics, Hi Resolution Graphics and Live Video.

H.264 HD System Flags

Content Settings	Flag Name	Range	Default
Graphics	H264_HD_GRAPHICS_MIN_CONTENT_RATE	0-1536	128
Hi Resolution Graphics	H264_HD_HIGHRES_MIN_CONTENT_RATE	0-1536	256
Live Video	H264_HD_LIVEVIDEO_MIN_CONTENT_RATE	0-1536	384

To change the System Flag default value, the flag must be manually added to the System Configuration. For more information see Modifying System Flags.

Example

The following table summarizes an example of two participants trying to connect to a conference running at a Line Rate of 1024Kbps. The Content Setting for the conference is **Hi Resolution Graphics** and the **H264_HD_HIGHRES_MIN_CONTENT_RATE** System Flag setting are used to determine if Content will be shared with the participant.

Participant Content Sharing Based on Connection Line Rate and System Flag Setting

	Participant		Confe	erence			
	Line Rate	Bit Rate Allocation to Content Channel	Line Rate	Bit Rate Allocation to Content Channel	Flag Value	Result	
Participant 1	384	192			128	Participant and entire conference share content at 192Kbps	
			1024	384	512	Participant receives content in the video channel (Legacy)	
Participant 2	1024	384	1024	364	128	Participant and entire conference share content at 384Kbps	
					512	Participant and entire conference share content at 384Kbps	

H.264 Cascade and SVC Optimized

The **H.264 Cascade and SVC Optimized** option maintains content quality and minimizes the amount of content refreshes that occur in large cascading conferences when participants connect or disconnect from the conference. uses fixed resolution and frame rate for SVC Only and mixed CP and SVC conferences. In AVC CP conferences, each content Line Rate and Content Setting has its own resolution and frame rate.

In AVC CP conferences - Endpoints that do not support the required content parameters (Content line rate, H.264 protocol and Content Resolution), along with ISDN endpoints, can be connected as Legacy Endpoints and receive content through their video channel. This ensures that Content settings are not changed following the participants connection or disconnection from the conference. If the **Send Content to Legacy Endpoints** option is disabled, these endpoints will not receive content.

In SVC Only conferences - Endpoints that do not support the required content parameters (Content line rate and Content Resolution) cannot share content.

Endpoints that do not support the required content parameters (Content line rate and Content Resolution) cannot share content.

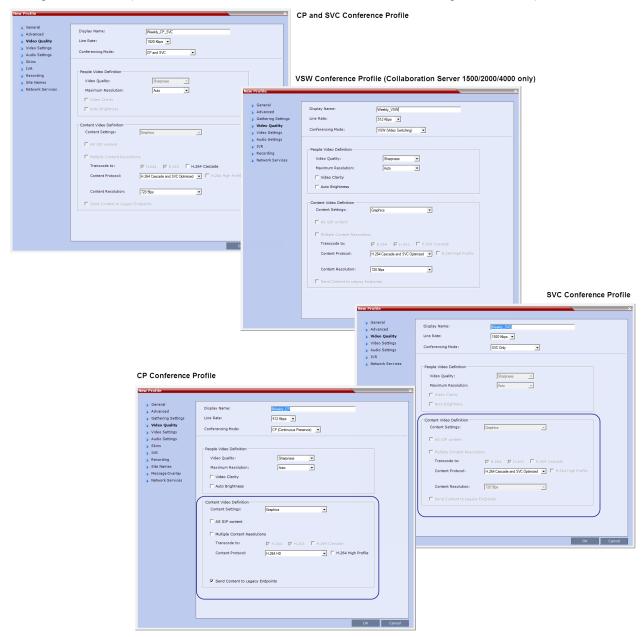
Guidelines for Sharing Content Using H.264 Cascade and SVC Optimized

- In Cascading conferences, the cascade link must be H.323.
- This is the only available Content sharing mode in SVC and mixed CP and SVC Conferencing Modes.
- In SVC and mixed CP and SVC Conferencing Modes the Content Line rate is fixed at 128Kbps.
- H.323, SIP and ISDN (Collaboration Server 1500/2000/4000) participants are supported in AVC CP Conferencing Mode.
- In Collaboration Server 1500/2000/4000, H.264 High Profile is not supported in MPMx Card Configuration Mode. H.264 High Profile is supported in MPMRx card Configuration Mode and with Collaboration Server 1800.
- Maximum supported content resolution is 1080p.
- When H.264 Cascade and SVC Optimized is selected in AVC CP Conferencing Mode, the Send Content to Legacy Endpoints selection is enabled by default. Endpoints that cannot connect at a line rate required to support the conference Content Rate are considered Legacy Endpoints and will receive Content in the video channel.
- In SVC Conferencing Mode, endpoints that cannot connect at a line rate required to support the conference Content Rate will receive Content in the video channel.
- Gathering Phase is not supported in Cascading Conferences.

Defining Content Sharing Parameters for a Conference

Content sharing parameters are defined in the Conference Profiles - Video Quality dialog box.

The available content options change according to the selected Conferencing Mode and the Card Configuration Mode (RMX 1500/2000/4000 MPMx and MPMRx Card Configuration Mode).



» In the Content Video Definition section, set the values for the Content Settings and Protocol as follows:

Content sharing Options

Field	Description
Content Settings	 Select the transmission mode for the Content channel: Graphics — basic mode, intended for normal graphics Hi-res Graphics (AVC CP Only) — a higher bit rate intended for high resolution graphic display Live Video (AVC CP Only) — Content channel displays live video Customized Content Rate (AVC CP Only) - manual definition of the Conference Content Rate, mainly for cascading conferences. Selection of a higher bit rate for the Content results in a lower bit rate for the people channel. For a detailed description of each of these options, see Content Sharing Parameters in Content Highest Common (Content Video Switching) Mode.
AS-SIP Content	AS-SIP is an implementation of SIP that utilizes SIP's built in security features. When selected, content is shared using the Multiple Resolutions mode and is not supported in any other Content sharing mode.
Multiple Resolutions	This Content Sharing option is available in CP Conferencing Mode only. Click this check box to enable the Multiple Content Resolutions mode, in which content is shared in multiple streams, one for each video protocol: H.263 and H.264. This allows endpoints with different protocols to connect and disconnect without having to restart Content sharing in the middle of a conference. When enabled, the H.264 is always selected and can not be deselected. Optional. Select additional protocols: H.263 - if the conference will include H.263-capable endpoints that do not support H.264 protocol for content sharing. H.264 Cascade - if the conference will include cascading links and you want to define the video settings for content sharing.
	Optional. If H.264 Cascade and SVC Optimized is selected, select the desired Content Resolution. For more information, see Sharing Content Using Multiple Content Resolutions Mode.

Content sharing Options

Field	Description
Content Protocol	 H.263 (AVC CP Only) Content is shared using the H.263 protocol. Use this option when most of the endpoints support H.263 and some endpoints support H.264. H.263 & H.264 Auto Selection (AVC CP Only) Content is shared using H.263 if a mix of H.263-supporting and H.264-supporting endpoints are connected. Content is shared using H.264 if all connected endpoints have H.264 capability. H.264 HD (AVC CP Only, default) Ensures high quality Content when most endpoints support H.264 and HD Resolutions. H.264 Cascade and SVC Optimized All Content is shared using the H.264 content protocol and is optimized for use in SVC only and Cascaded Conferences. For a detailed description of each of these settings, see Content Protocols.
Content Resolution	Select a Content Resolution from the drop-down menu. The Content Resolutions that are available for selection are dependent on the content sharing mode (Highest Common Content or Multiple Content Resolutions), Line Rate and Content Settings that have been selected for the conference. For a full list of Content Resolutions see Defining Content Sharing Parameters for a Conference. Note: This field is displayed only when H.264 Cascade and SVC Optimized is selected for Multiple Content Resolution or when H.264 Cascade and SVC Optimized option is selected as the Content Protocol (in the Highest Common Content Mode) and is enabled for selection in CP conferences (AVC CP Only). This option is disabled in SVC conferences.
Send Content to Legacy Endpoints	When enabled (default), Content can be sent to H.323/SIP (Collaboration Server 1500/1800/2000/4000) or ISDN (Collaboration Server 1500/2000/4000 only) endpoints that do not support H.239 Content (legacy endpoints) over the video (people) channel. For more information see Sending Content to Legacy Endpoints (AVC Only).

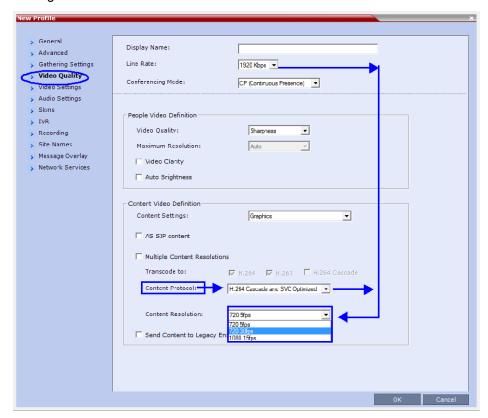
Enabling H.264 Cascade and SVC Optimized Content Sharing in AVC CP Conferences

When **H.264 Cascade and SVC Optimized** is selected in AVC CP conference as the Content Protocol, an additional field, **Content Resolution** is displayed in the **Content Video Definition** pane.

In SVC Conferencing Mode and CP and SVC Conferencing Mode, the Content Resolution option is disabled.

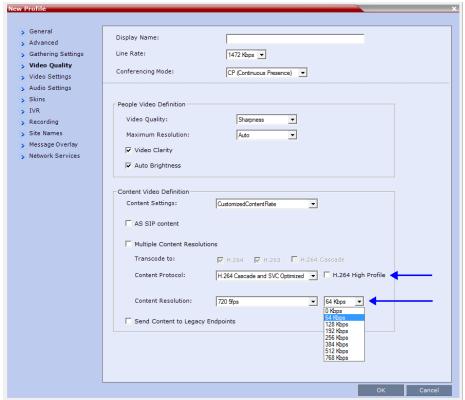
The Content Resolution is a fixed resolution and frame rate for Content sharing in a Cascaded Conference.

The **Content Resolutions** that are available for selection are dependent on the Line Rate and Content Settings that have been selected for the conference.



AVC CP Conferencing Mode

An additional check box **H.264 High Profile** and an additional **Content Rate** drop-down menu are displayed in the **Video Quality** dialog box if the conditions listed below are satisfied.



The **H.264 High Profile** check box is un-checked by default and is displayed next to the **Content Protocol** drop-down menu if all the following conditions are met:

- The MCU is a RealPresence Collaboration Server 1800, or 2000/4000 containing MPMRx cards.
- The selected Conferencing Mode is AVC-CP.
- Multiple Resolutions (Content Transcoding) is not selected.
- The selected Content Protocol is H.264 HD, H.264 Cascade and SVC Optimized, or H.263 and H.264 Auto Selection.

If H.264 HD, H.264 Cascade and SVC Optimized is selected, the Content Resolution is set according to the line rate.

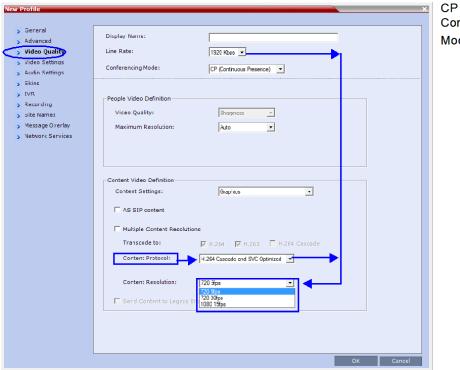
If **H.263 and H.264 Auto Selection** is selected, the **Content Resolution** is automatically set according to the line rate, and the **H.264 High Profile** check box is automatically unchecked and disabled.

- TIP Compatibility (in the Profile Advanced dialog box) is selected as None or Video Only.
- The conference Line Rate is sufficient to support HD1080p30/60 content.

The Content Rate drop-down menu is displayed next to the Content Resolution drop-down menu when:

- H.264 Cascade and SVC Optimized is the selected Content Protocol and
- Customized Content Rate is the selected Content Setting.

The Content Rate is dependent on the MCU type (RealPresence Collaboration Server with MPMRx or RealPresence Collaboration Server 1800) and can be up to 66% of the conference line rate. In MCUs with MPMRx cards the Content Rate is limited to 2048 kbps, while when used with the RealPresence Collaboration Server 1800 the Content Rate is limited to 4096 kbps.



CP Conferencing Mode§

The following tables summarize the interaction of these parameters for Base Profile and High Profile settings.

For more information see H.264 Base Profile and High Profile Comparison.

Bit Rate Allocation to Content Channel per Conference Line Rate for H.264 Cascade and SVC Optimized for Base Profile

	Cor	ntent B	it Rate	Alloca	ation p	er Con	ference	Line R	ate (Kbp	s)						
	64	128	256	384	512	768	832	1152	1280	1472	1920	2048	3072	3584	4096	6144
	96	192	320				1024			1536		2560				
										1728						
Cascade F	Resol	ution														
Graphics																
720p5		64	64	128	128	256	256	256	256	256	256	512	512	512	512	512
720p30		•	•	•	•	•		•	•	512	512	512	512	512	512	768
1080p15										•	768	768	768	1152	1152	1152
1080p30														•	•	2048
1080p60																
Hi-res Gra	phic	5														
720p5		64	128	192	256	384	384	384	512	512	512	512	512	512	512	512
720p30			•		•	•		512	512	512	512	768	768	768	768	768
1080p15								•		768	768	768	768	768	1152	1152
1080p30															2048	2048
1080p60															•	3072
Live Video	,															
720p5		64	128	256	384	512	512	768	768	768	768	768	768	768	768	768
720p30							512	768	768	768	768	768	768	768	768	768
1080p15								768	768	768	768	1152	1152	1152	1152	1152
1080p30									•	•		•	2048	2048	2048 ‡	2048
1080p60													•			4096

Bit Rate Allocation to Content Channel per Conference Line Rate for H.264 Cascade and SVC Optimized for High Profile

	Con	tent Bi	it Rate	Alloca	tion pe	r Conf	erence	Line Ra	ate (Kbp	s)						
	64	128	256	384	512	768	832	1024	1152	1536	1728	1920	2048	2560	4096	6144
	96	192	320						1280					3072		
									1472					3584		
Cascade I	Cascade Resolution															
Graphics																
720p5		64	64	128	128	256	256	256	384	384	512	512	512	512	512	512
720p30									384	512	512	512	512	768	768	768
1080p15		512 512 512 512 768									768	1280	1280			
1080p30	768									1280	2048					
1080p60	0										2048					
Hi-res Gra	phics	•														
720p5		64	128	192	256	384	384	384	512	512	512	512	512	512	512	512
720p30						384	384	512	512	768	768	768	768	768	768	768
1080p15								512	512	768	768	768	768	1280	1280	1280
1080p30										768	768	768	1024	1024	2048	2048
1080p60															2048	3072
Live Video	•															
720p5		64	128	256	256	384	512	512	512	512	512	512	512	512	512	512
720p30						512	512	512	768	768	768	768	768	768	768	768
1080p15						512	512	512	768	768	768	1280	1280	1280	1280	1280
1080p30	768 1024 1024 1280 1280 1280										2048	2048				
1080p60															2560	4096

The selection of the appropriate Content Resolution option, when several options are available, should be based on the line rate and capabilities that can be used by most or all endpoints connecting to the conference.

Examples:

- If the conference Line Rate is 1024 kbps.
 and
- If the Content Settings selection is **Graphics**.
 - ➤ Content Resolutions of HD720/5 and HD1080/15 are selectable with 256 kbps and 768 kbps allocated as the Conference Content Rate, respectively.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)										
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144		
	HD720/5		64	128	128	256	256	256	512	512		
Graphics	HD720/30							512	512	512		
	HD1080/15						768	768	1152	1152		

The higher Content Resolution, **HD1080/15** should be selected only if most of the endpoints connecting to the conference can support a Content Rate of 768Kbps, which requires the participant to connect to the conference at a Line Rate of 1024kbps.

When the lower Content Resolution **HD720/5** is selected, the conference Content Rate is set to 256 kbps. This will enable the endpoints that connect to the conference at a Line Rate of at least 768 kbps to receive content in the Content channel. Endpoints that connect to the conference at a line rate lower than 768Kbps, will receive content in the video channel.

- If the Content Settings selection is Hi Resolution Graphics.
 - Only HD720/5 can be selected as the Content Resolution with 384 kbps allocated as the conference Content Rate.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)										
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144		
	HD720/5			192	256	384	384	512	768	512		
Hi Resolution Graphics	HD720/30							512	768	768		
	HD1080/15								768	1152		

Only endpoints that connect at a Line Rate of 1024 kbps that is required to support a Content Rate of 384 kbps will receive content in the Content channel. Endpoints that connect to the conference at a line rate lower than 1024 kbps, will receive content in the video channel will not receive content.

- If the Content Settings selection is Live Video.
 - ➤ HD720/5, HD720/30 or HD1080/15 can be selected as the Content Resolution with 768 kbps allocated the as the Conference Content Rate.

Content Settings	Cascade Resolution/ fps	Content Bit Rate Allocation per Conference Line Rate (kbps)										
		64 96	128 256	384	512	768 823	1024 1152	1472 1728 1920	2048	4096 6144		
Live Video	HD720/5			256	384	512	768	768	768	768		
	HD720/30					512	768	768	768	768		
	HD1080/15						768	768	1152	1152		

The higher Content Resolution should be selected according to the resolution capabilities of the majority of the endpoints connecting to the conference. Endpoints that cannot support the selected Content Resolution are considered Legacy Endpoints and will receive Content in the video channel.

Selecting a Customized Content Rate in AVC CP Conferences

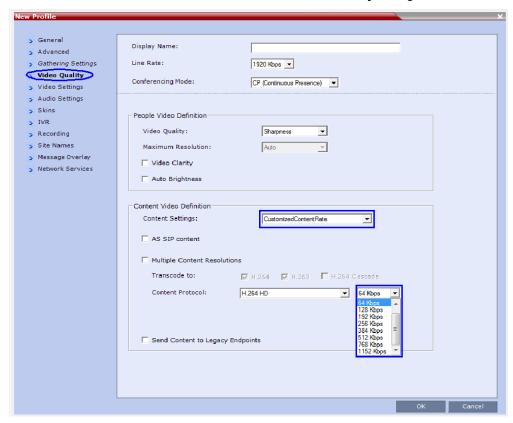
Customized Content Rate functionality can be implemented when a Conference Content Rate, that is automatically calculated by the Collaboration Server, may not be suitable in a Cascaded Environment, where conference line rates may vary widely between the cascaded conferences. For example, one conference may have a line rate of 2 Mbps, and the other a line rate of is 512kbps.

Guidelines for Selecting a Customized Content Rate

- Cascaded conferences may have different Conference Line Rates.
- The Customized Content Rate must be the same for all cascaded conferences.

To Select the Customized Content Rate:

Customized Content Rate is enabled in the Profile - Video Quality dialog box.



1 In the Content Settings list, select Customized Content Rate.

When selected, a drop-down menu of the available Conference Content Rates is displayed. These Content Line Rates are based on and will vary according to the selected Conference Line Rate.

The largest selectable Content Line Rate is 66% of the Conference Line Rate.

If the Conference Line Rate is 64kbps or 96kbps, the only available Conference Content Rate is 0, indicating that Content is not supported at these rates.

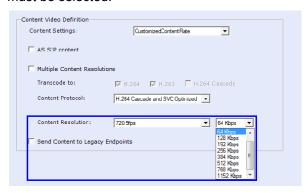
2 Select the required content rate.

When selecting a Conference Line Rate (after selecting Customized Content Rate) that is too low for the selected Customized Content Rate, the following error message is displayed:

The selected Conference Line Rate is too low to support the selected Content Line Rate. Click Cancel and reconfigure either of the Line Rates or click OK to return to the default Content Setting.

You can then modify either the Content Line Rate or the Conference Line Rate or select another Content Setting option.

3 If H.264 Cascade and SVC Optimized is the selected Content Protocol, a Content Resolution must be selected.



(If CP and SVC Conferencing Mode is selected, the Content Line Rate is fixed at 128Kbps.).

The following table lists the Cascade Resolutions available for the various Conference Content Rates.

H.264 Cascade and SVC Optimized - Cascade Resolutions

H.264 Cascade Optimized									
Conference Content Rate (Kbps)	Available Resolutions*								
64	HD720p5 Content Not Supported								
128	HD720p5								
192	HD720p5								
256	HD720p5								
384	HD720p5								
512	HD720p5	HD720p30							
768	HD720p5	HD720p30	HD1080p15						
1152	HD720p5	HD720p30	HD1080p15						
1536	HD720p5	HD720p30	HD1080p15						

H.264 Cascade and SVC Optimized - Cascade Resolutions

H.264 Cascade Optimi	H.264 Cascade Optimized									
Conference Content Rate (Kbps)	Available Resolutions*									
64	HD720p5 Content Not Supported									
128	HD720p5									
192	HD720p5									
256	HD720p5									
384	HD720p5									
512	HD720p5	HD720p30								
768	HD720p5	HD720p30								
1152	HD720p5	HD720p30								
1536	HD720p5	HD720p30								
2048	HD720p5	HD1080p30 HD1080p60								

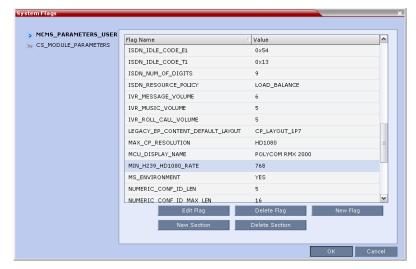
^{*}The default resolution for all Content Rates is **HD720p5**.

Modifying the Threshold Line Rate for HD Resolution Content

The threshold line rate for HD Resolution Content is the line rate at which the Collaboration Server will send Content at HD1080 Resolution. The default is 768 kbps. When the threshold value is set to 0, HD720p/HD1080p resolutions for Content sharing are disabled.

To modify the HD Resolution Content threshold line rate:

1 On the Collaboration Server menu, click Setup > System Configuration. The System Flags dialog box opens.



2 In the MCMS_PARAMETERS tab, double-click the MIN_H239_HD1080_RATE entry.

The **Update Flag** dialog box is displayed.

- 3 In the **Value** field, enter the minimum line rate at which HD1080 Resolution Content will be enabled. Enter **0** to disable this flag and prevent HD Content from being used.
- 4 Click **OK** to confirm and exit the **Update Flag** dialog box.
- 5 Click Close to exit the System Flags dialog box.

Sharing Content Using Multiple Content Resolutions Mode



Multiple Content Resolutions option is not supported in Ultra Secure Mode.

In Multiple Content Resolutions mode, content is shared in multiple streams, one for each video protocol: H.263 and H.264. This allows endpoints with different protocols to connect and disconnect without having to restart Content sharing in the middle of a conference.

Guidelines for Sharing Contents using Multiple Content Resolutions

- Multiple Content Resolutions is supported only in VC CP conferences.
- When Multiple Content Resolutions is enabled, Content is always provided to H.264 HD endpoints. Resolutions of HD720p30 and HD1080p15 are supported.
- When Multiple Content Resolutions is enabled, the **Send Content to Legacy Endpoints** option is selected and cannot be modified.
- Additional resources are allocated to the conference (in addition to the resources occupied by the conference participants) for processing the content:
 - Resources are allocated only when content sharing is started.

- If only HD720p30 content is provided, 1.5 HD video resources are allocated to the conference.
- ➤ If HD1080p15 is provided, 2 HD video resources are allocated to the conference.
- Optionally, content can be sent at multiple resolutions to H.263 endpoints and H.264 endpoints whose resolution is lower than HD and support H.263 content. In this case an additional resource is allocated.
- Optionally, content can be sent to cascaded RealPresence Collaboration Servers.
 - > An additional resource is allocated to the conference, based on the content resolution selected. The resolution sent is set in the Conference Profile when H.264 Cascade is selected.
 - All cascading conferences must be defined with the same content settings (content line rate, resolution and frame rate).
 - A link that does not support the content settings cannot receive content.
- If there are not enough resources available, Multiple Content Resolutions is disabled and the conference does not include cascading links, content sharing mode reverts to Content Video Switching mode.

If the conference includes cascading links, and the conference is set to H.264 Cascade and SVC Optimized:

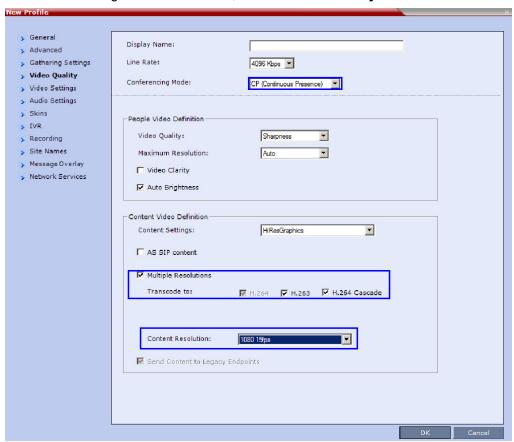
- ➤ H.264-capable endpoints will share content using these settings.
- H.263-capable endpoints will not share content and will receive the content over the video (people) channel.
- If H.264 Cascade was not selected for the conference, the H.264 HD protocol will be used.
- H.264 endpoints that are not HD capable and do not support H.263 will receive content over the video (people) channel.
- TIP endpoints are not supported. Content will be displayed over the video (people) channel.
- If AS SIP is enabled for the conference, Multiple Resolutions will be checked. H.264 will be enabled, and both H.263 and H.264 Cascade will be hidden. This can improve AS SIP performance in high-traffic environments. In this case, resources are allocated immediately when the conference is started.

Enabling Multiple Content Resolutions for Content Sharing

The Multiple Content Resolutions mode can be modified in the conference Profile, in the Video Quality Tab.

To enable Multiple Content Resolutions:

1 In a new or existing Conference Profile, click the Video Quality tab.



- 2 If the Conference Mode is not CP (Continuous Presence), select CP.
- 3 Select the Multiple Resolutions check box.
 - By default, **H.264** is always selected and can not be modified.
- 4 Optional. Select additional protocols:
 - ➤ **H.263** if the conference will include H.263-capable endpoints that do not support H.264 protocol for content sharing.
 - ➤ **H.264 Cascade** if the conference will include cascading links and you want to define the video settings for content sharing.
 - Optional. If H.264 Cascade is selected, select the Content Resolution.
- 5 Click Ok.

Sending Content to Legacy Endpoints (AVC Only)

The Collaboration Server can be configured to send Content to IP (H.323/SIP) or ISDN (Collaboration Server 1500/2000/4000) endpoints that do not support H.239 Content (legacy endpoints) over the video (people) channel, allowing the participants using legacy endpoints to view Content instead of the other conference participants.

Guidelines for Sending Content to Legacy Endpoints

- This option is valid when sending Content as a separate stream is enabled in the System Configuration and the flag: ENABLE_H239 is set to YES.
- One additional HD video resource is allocated to the conference when Content is sent to legacy endpoints.

The allocation is done only when a legacy endpoint is connected to the conference and a Content session is initiated and transmitted via the video channel. Once the resource is allocated, it remains allocated to the conference until the conference ends.

If the system cannot allocate the resource required for sending the Content, the conference status changes to **Content Resource Deficiency**, and Content will not be sent to the legacy endpoints.

As the resource required for sending Content to legacy endpoints is allocated on the fly, when scheduling a reservation, in rare occasions when the MCU is fully loaded, Resource deficiency may be encountered. This may prevent participants from connecting to the conference or from Content being sent to the legacy endpoint. To ensure resource for sending Content to legacy endpoints, add one resource to the number of resources defined in the Reserve Resources for Video Participants field, in the **Conference Properties - General** dialog box.

- H.323, SIP, ISDN, and Telepresence non-H.239 (legacy) endpoints receive the Content via the video channel using the same video protocol and resolution with which they receive video.
- The highest content resolution for legacy endpoints is: **HD720p30**.
- Once an endpoint is categorized as a Legacy Endpoint and receives the content over the video channel, it remains in this mode without the ability to receive content over the Content channel.
- Content cannot be sent to legacy endpoints when Same Layout mode is selected for the conference.
- This option in not supported in Video Switching conferences.
- When content is transmitted, the Site Name of the endpoints cannot be viewed.
- Content can be sent to legacy endpoints in gateway calls.
- When moving a legacy participant to the Operator conference, content will not be available to the legacy endpoint.
- A Polycom FX endpoint dialing in to a Collaboration Server with MPMx cards will receive content
 using People + Content. An FX endpoint dialed out from a Collaboration Server with MPMx cards will
 only receive content via the video channel using People + Content if Send Content to Legacy
 Endpoints is enabled in the Conference Profile.

Content Display on Legacy Endpoints

When Contents is sent to legacy endpoints, their video layout automatically changes to a Content Layout which is defined by the system flag **LEGACY_EP_CONTENT_DEFAULT_LAYOUT** and the Content is shown in the larger/top left (speaker) window. The video layouts of the other conference participants do not change.

The switch to the Content layout occurs in the Auto Layout, Presentation Mode, Lecture Mode and when a layout is selected for the conference. However, in Lecture Mode, when Content is sent to legacy endpoints, when switching to the Content layout, the Content is shown in the lecturer/speaker window and the lecturer is shown in a second window. If the layout contains more than two windows, all other windows will be empty. All other participants will see the lecturer in full screen.

In Same Layout mode, Content cannot be sent to legacy endpoints.

The **LEGACY_EP_CONTENT_DEFAULT_LAYOUT** Flag default is set to a layout of 1+4 where the Content is shown in the large window and the other conference participants are shown in the small windows. This default value can be changed in the System Configuration.

When Content is stopped, the layout of the legacy participants returns to the last video layout seen prior to the Content mode.

The Legacy participants can change their layout using Click&View. In such a case, the Content is forced to the speaker window.

The Collaboration Server user can also change the layout for the participants the legacy endpoints (selecting personal layout).

When forcing a video participant to the Content window (instead of Content), the Content display can be restored only by selecting any other video layout.

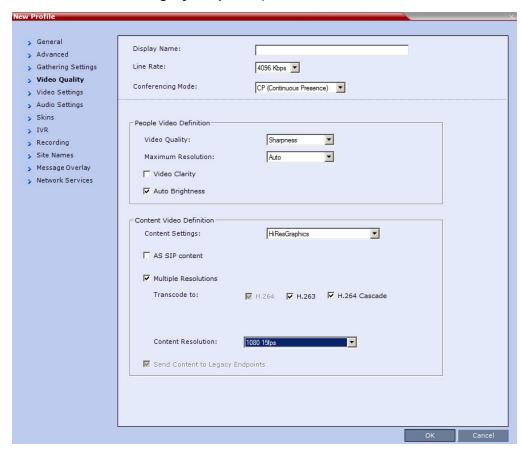
Interoperability with Polycom CMA and RealPresence DMA System

The CMA uses the Profiles that are stored in the Collaboration Server. If the **Send Content to Legacy Endpoints** option is enabled in the Conference Profile, this option will be enabled in the conference started from the CMA that uses that Profile. However, the CMA does not display an indication that this option is enabled for the conference.

A new conference can be started on the RealPresence DMA System using a Conference Profile that is defined on the Collaboration Server or by defining all the conference parameters. The **Send Content to Legacy Endpoints** option can be enabled only in the Conference Profile defined in the Collaboration Server, therefore, to include this option in the conference started on the DMA use an Collaboration Server existing Profile. However, the DMA does not display an indication that this option is enabled for the conference.

Enabling the Send Content to Legacy Endpoints Option

The Send Content to Legacy Endpoint option is enabled in the Conference Profile - Video Quality tab.



If the Conferencing Mode is set to **Video Switching**, the **Send Content to Legacy Endpoints** option is disabled.

If the Same Layout option is selected in the Conference Profile - Video Settings tab, the Send Content to Legacy Endpoints option is disabled.



Select this option when Avaya IP Softphone will be connecting to the conference.

Changing the Default Layout for Displaying Content on Legacy Endpoints

The default layout that will be used to display Content on the screens of legacy endpoints is defined by the system flag **LEGACY_EP_CONTENT_DEFAULT_LAYOUT**.

The configured default layout is **1+4** (**CP_LAYOUT_1P4VER**). You can change the default layout configuration by entering a new value for the flag in the system configuration.

To modify System Flags:

- 1 On the Collaboration Server menu, click **Setup > System Configuration**.
 - The **System Flags** dialog box opens.
- 2 In the MCMS_PARAMETERS tab, double-click the LEGACY_EP_CONTENT_DEFAULT_LAYOUT entry.
 - The **Edit Flag** dialog box is displayed.
- 3 In the **Value** field, enter the flag value for the required layout as follows:

LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values

Layout	Flag Value
	CP_LAYOUT_1X1
	CP_LAYOUT_1X2
	CP_LAYOUT_1X2HOR
	CP_LAYOUT_1X2VER
=	CP_LAYOUT_2X1
	CP_LAYOUT_1P2HOR
	CP_LAYOUT_1P2HOR_UP
08	CP_LAYOUT_1P2VER
	CP_LAYOUT_2X2
	CP_LAYOUT_1P3HOR_UP
	CP_LAYOUT_1P3VER
	CP_LAYOUT_1P4HOR_UP
0000	CP_LAYOUT_1P4HOR
	CP_LAYOUT_1P4VER
	CP_LAYOUT_1P5

LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values

Layout	Flag Value
	CP_LAYOUT_1P7
	CP_LAYOUT_1P8UP
0000	CP_LAYOUT_1P8CENT
000	CP_LAYOUT_1P8HOR_UP
	CP_LAYOUT_3X3
	CP_LAYOUT_2P8
0000 0000	CP_LAYOUT_1P12
0000	CP_LAYOUT_4X4

4 Click OK.

The flag is updated in the MCMS_PARAMETERS list.

5 Click OK.



For flag changes (including deletion) to take effect, reset the MCU. For more information see Resetting the RMX.

Sending Content to Legacy Endpoints in Telepresence Mode

The Collaboration Server can be configured to manage the layouts of to H.323/SIP/ISDN endpoints that do not support H.239 Content (legacy endpoints) over the video (people) channel in Telepresence conferences when Content is being sent.

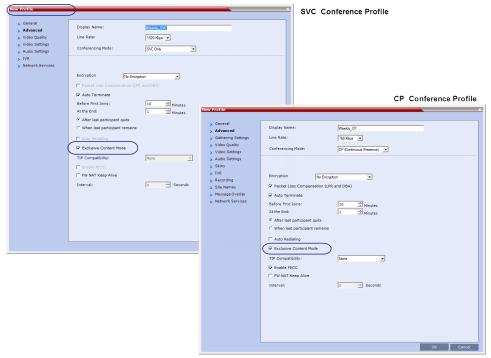
For more information, see Sending Content to Legacy Endpoints in Telepresence Mode.

Exclusive Content Mode

In this mode, Content broadcasting is limited to one participant, preventing other participants from interrupting the Content broadcasting while it is active.

Guidelines for Sharing Content in Exclusive Content Mode

- Exclusive Content Mode is available in all Conferencing Modes.
- The Exclusive Content Mode is enabled or disabled (system default) by a check box in the in the
 Conference Profile Advanced dialog box or during the ongoing conference using the Conference
 Properties Advanced dialog box.



- In Exclusive Content Mode, if the **RESTRICT_CONTENT_BROADCAST_TO_LECTURER** system flag is set to:
 - NO The first participant to send content becomes the Content Token holder and has to release the Content Token before any other participant can acquire the token and begin transmitting Content.
 - > YES Only the designated Lecturer can be the Content Token holder.
- The Exclusive Content Mode check box replaces the EXCLUSIVE_CONTENT_MODE system flag
 which was used to control exclusive content mode for the system in previous versions.
- In Exclusive Content Mode, if an endpoint attempts to send Content a few seconds after another
 endpoint sent Content, the Content stream it is receiving is momentarily interrupted by a slide which
 is displayed for a few seconds before the normal Content stream is resumed.

Stopping a Content Session

In some cases, when one participant ends the Content session from his/her endpoint, the Content token is not released and other participants cannot send Content.

The Collaboration Server User can withdraw the Content token from the current holder and to return it to the MCU for assignment to other endpoints.

To end the current Content session:

» In the Conferences list pane, right-click the conference icon and then click Abort H.239 Session.



Content Broadcast Control

Content Broadcast Control prevents the accidental interruption or termination of H.239 Content that is being shared in a conference.

Content Broadcast Control achieves this by giving Content Token ownership to a specific endpoint via the Collaboration Server Web Client. Other endpoints are not able to send content until Content Token ownership has been transferred to another endpoint via the Collaboration Server Web Client.

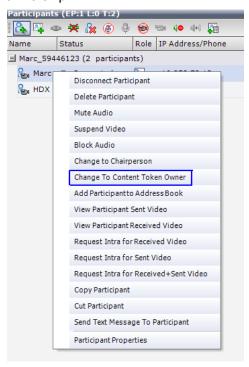
Guidelines for Controlling Content Broadcast

- Content Broadcast Control is supported in CP and Video Switching conferences.
- Content Broadcast Control is supported in H.323 environments.
- Only the selected Content Token owner may send content and Content Token requests from other endpoints are rejected.
- Content Token ownership is valid until:
 - > It is canceled by the Collaboration Server User via the Collaboration Server Web Client.
 - The owner releases it.
 - > The endpoint of the Content Token owner disconnects from the conference.
- The Collaboration Server User can cancel Content Token ownership.
- In cascaded conferences, a participant functioning as the cascade link cannot be given token ownership.

Giving and Cancelling Token Ownership (AVC Participants)

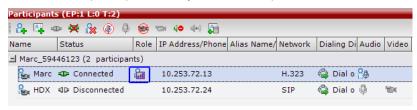
To give token ownership:

1 In the **Participants** list, right click the AVC-enabled endpoint that is to receive Content Token ownership.



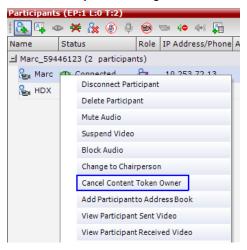
2 Select Change To Content Token Owner in the drop-down menu.

The endpoint receives ownership of the Content Token and an indication icon is displayed in the Role column of the participant's entry in the Participants list.



To cancel token ownership:

1 In the Participants list, right click the endpoint that currently has Content Token ownership.



2 Select Cancel Content Token Owner in the drop-down menu.

Content Token ownership is cancelled for the endpoint.

Forcing Other Content Capabilities

The **H239_FORCE_CAPABILITIES** system flag in **system.cfg** gives additional control over Content sharing:

- When the flag is set to NO (default), the Collaboration Server only verifies that the endpoint supports the content protocols: H.263 or H.264.
- When set to YES, the Collaboration Server checks frame rate, bit rate, resolution, annexes and all
 other parameters of the Content mode as declared by an endpoint during the capabilities negotiation
 phase. If the endpoint does not support the Content capabilities of the MCU, the participant will not
 be able to send or receive content over a dedicated content channel.

Content Sharing via the Polycom CCS Plug-in for Microsoft Lync Clients

From version 8.1, Polycom CCS (Content Collaboration Solution) Plug-in for Lync clients allows Lync clients to receive and send Content on a separate channel, without having to use the video channel. Content is transmitted using SIP BFCP.

For more information, see Sharing Content Using Multiple Content Resolutions Mode.

Managing Noisy Content Connections

The system can identify participants who send frequent requests to refresh their Content display usually as a result of a problematic network connection. The frequent refresh requests cause frequent refresh of the Content display and degrade the viewing quality.

When the system identifies the noisy participants, the system will automatically suspend the requests to refresh the sent Content to avoid affecting the quality of the Content viewed by other conference participants. This process is controlled by System flags.

Content Display Flags

MAX_INTRA_REQUESTS_PER_INTERVAL_CONTENT

Enter the maximum number of refresh (intra) requests for the Content channel sent by the participant's endpoint in a 10 seconds interval that will be dealt by the Collaboration Server system. When this number is exceeded, the Content sent by this participant will be identified as noisy and his/her requests to refresh the Content display will be suspended.

Default setting: 3

MAX_INTRA_SUPPRESSION_DURATION_IN_SECONDS_CONTENT

Enter the duration in seconds to ignore the participant's requests to refresh the Content display. Default setting: **10**

CONTENT_SPEAKER_INTRA_SUPPRESSION_IN_SECONDS

This flag controls the requests to refresh (intra) the Content sent from the Collaboration Server system to the Content sender as a result of refresh requests initiated by other conference participants.

Enter the interval in seconds between the Intra requests sent from the Collaboration Server to the endpoint sending the Content to refresh the Content display. Refresh requests that will be received from endpoints within the defined interval will be postponed to the next interval.

Default setting: 5

Implementing Media Encryption for Secured Conferencing

Encryption is available at the conference and participant levels, based on AES 128 (Advanced Encryption Standard) and is fully H.233/H.234 compliant and the Encryption Key exchange DH 1024-bit (Diffie-Hellman) standards.

Media Encryption Guidelines

- Encryption is not available in all countries and it is enabled in the MCU license. Contact Polycom Support to enable it.
- Media encryption is supported in CP, SVC Only and mixed CP and SVC Conferencing Modes.
- Endpoints must support both AES 128 encryption and DH 1024 key exchange standards which are compliant with H.235 (H.323) to encrypt and to join an encrypted conference.
- The encryption mode of the endpoints is not automatically recognized, therefore the encryption mode must be set for the conference or the participants (when defined).
- Media Encryption for ISDN/PSTN participants is implemented in Collaboration Server 1500/2000/4000 systems and is not supported in cascaded conferences.
- Conference level encryption must be set in the Profile, and cannot be changed once the conference is running.
- If an endpoint connected to an encrypted conference stops encrypting its media, it is disconnected from the conference.
- In Cascaded conferences, the link between the cascaded conferences must be encrypted in order to encrypt the conferences.
- The recording link can be encrypted when recording from an encrypted conference to the RSS that is set to encryption. For more information, see Recording Link Encryption.
- Encryption of SIP Media is supported using SRTP (Secured Real-time Transport Protocol) and the AES key exchange method.
- Encryption of SIP Media requires the encryption of SIP signaling TLS Transport Layer must be used.
- Encryption of SIP Media is supported in conferences as follows:
 - All media channels are encrypted: video, audio and FECC.
 - > Collaboration Server SRTP implementation complies with Microsoft SRTP implementation.
 - > LPR is not supported with SRTP.
 - ➤ The ENABLE_SIRENLPR_SIP_ENCRYPTION System Flag enables the SirenLPR audio algorithm when using encryption with the SIP protocol. The default value of this flag is NO meaning SirenLPR is disabled by default for SIP participants in an encrypted conference. To enable SirenLPR the System Flag must be added to system.cfg and its value set to YES.

> The **SEND_SRTP_MKI** System Flag enables or disables the inclusion of the MKI field in SRTP packets sent by the Collaboration Server. The default value of the flag is **YES**.

Add the flag to **system.cfg** and set its value set to **NO** to disable the inclusion of the MKI field in SRTP packets sent by the Collaboration Server when using endpoints that cannot decrypt SRTP-based audio and video streams if the MKI (Master Key Identifier) field is included in SRTP packets sent by the Collaboration Server. When all conferences on the RMX will not have MS-Lync clients participating and will have 3rd party endpoints participating. This setting is recommended for Maximum Security Environments.

Add the flag to **system.cfg** and set its value set to **YES** when Microsoft Office Communicator and Lync Clients. When any conferences on the RMX will have both MS-Lync clients and Polycom endpoints participating. Some 3rd party endpoints may be unsuccessful in participating in conferences with this setting.

Polycom endpoints function normally regardless of the setting of this flag.

For more information, see Modifying System Flags.

• In compliance with UC_APL_SEC_0013, the Collaboration Server 1500/2000/4000 supports an additional Privacy Protocol AES_CM_128_HMAC_SHA1_32, in addition to AES_CM_128_HMAC_SHA1_80. For more information see Media Encryption and Authentication.

Mixing Encrypted and Non-encrypted Endpoints in one Conference

Mixing encrypted and non-encrypted endpoints in one conference is possible, based on the Encryption option **Encrypt When Possible** in the **Conference Profile - Advance** dialog box. The behavior is different for H.323/SIP and ISDN participants (Collaboration Server 1500/2000/4000).

In Collaboration Server 1500/2000/4000 with versions prior to version 7.6.1, this behavior is based on the setting of the system flag **ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF**.

The option **Encrypt When Possible** enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. Defined participants that cannot connect encrypted are connected non-encrypted, with the exception of dial-out SIP participants.



- When the conference encryption is set to Encrypt when possible, SIP dial out participants
 whose encryption is set to AUTO can only connect with encryption, otherwise they are
 disconnected from the conference.
- In CISCO TIP environments, dial in endpoints that are registered to CUCM can only connect as non-encrypted when the conference encryption is set to Encrypt when possible as the CUCM server sends the Invite command without SDP.

The same system behavior can be applied to undefined participants, depending on the setting of the System Flag FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE:

- When set to NO and the conference encryption in the Profile is set to Encrypt when possible, both Encrypted and Non-encrypted undefined participants can connect to the same conferences, where encryption is the preferred setting.
- When set to YES (default), Undefined participants must connect encrypted, otherwise they are disconnected.

For defined participants, connection to the conference is decided according to the encryption settings in the conference Profile, the Defined Participant's encryption settings.

For undefined participants, connection to the conference is decided according to the encryption settings in the conference Profile, the System Flag setting and the connecting endpoint's Media Encryption capabilities.

Direct Connection to the Conference

The following table summarizes the connection status of participants, based on the encryption settings in the conference Profile, the Defined Participant's encryption settings or the System Flag setting for undefined participants and the connecting endpoint's Media Encryption capabilities.

Connection of Participants to the Conference based on Encryption Settings

Conference	D	efined Participant	Undefined	Participant		
Encryption Setting	Encryption Setting	Connection status	Connection Status *Flag = No	Connection Status *Flag = YES		
No Encryption	ption Auto Connected, non-encrypted		Connected non-encrypted	Connected non-encrypted		
	No	Connected, non-encrypted	(Encryption is not declared by the Collaboration	(Encryption is not declared by the Collaboration		
	Yes	Connected only if encrypted. Non-encrypted endpoints are disconnected as encryption is forced for the participant.	Server, therefore the endpoint does not use encryption)	Server, therefore the endpoint does not use encryption)		
Encrypt All	Auto	Connected, encrypted. Non-encrypted endpoints are disconnected	Connect only if encrypted. Non-encrypted	Connect only if encrypted. Non-encrypted endpoints are disconnected		
	No	Disconnected (cannot be added to the conference)	endpoints are disconnected			
	Yes	Connected, encrypted				

Connection of Participants to the Conference based on Encryption Settings

Conference	Defined Participant		Undefined Participant	
Encryption Setting	Encryption Setting	Connection status	Connection Status *Flag = No	Connection Status *Flag = YES
Encrypt When Possible	Auto	All defined participants except dial-out SIP participants: Connect encrypted - Endpoints with encryption capabilities. Connect non-encrypted - endpoints without encryption capabilities. Defined dial-out SIP participant: Connect only if encrypted. Non-encrypted endpoints are disconnected.	Connect encrypted - Endpoints with encryption capabilities. Connect non-encrypted - endpoints without encryption capabilities	Connect only if encrypted. Non-encrypted endpoints are disconnected.
	No Connected, non-encrypted Yes Connected, encrypted			

^{*} System Flag =

FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE

Connection to the Entry Queue

An undefined participant connecting to an Entry Queue inherits the encryption characteristics of the Entry Queue as defined in the Entry Queue's profile.

Participants can be moved from the Entry Queue and the destination conference if both conferencing entities have the same Profile settings, i.e. from SVC Only Entry Queue to SVC Only conference and from mixed CP and SVC Entry Queue to a mixed CP and SVC conference, etc.

The following table summarizes the connection possibilities for a participant that is to be moved from an Entry Queue to a destination conference for each of the conference Profile and Entry Queue encryption options.

Connection of Undefined Participants to the Entry Queue Based on Encryption Settings

Entry Queue Encryption	Undefined Participant Connection to the Entry Queue		
Setting	*Flag = No	*Flag = YES	
No Encryption	Connected, non-encrypted (Encryption is not declared by the Collaboration Server, therefore endpoint does not use encryption)	Connected, non-encrypted (Encryption is not declared by the Collaboration Server, therefore endpoint does not use encryption)	

Connection of Undefined Participants to the Entry Queue Based on Encryption Settings

Entry Queue Encryption	Undefined Participant Connection to the Entry Queue		
Setting	*Flag = No	*Flag = YES	
Encrypt All	Connected only if encrypted. Non-encrypted endpoints are disconnected	Connected only if encrypted. Non-encrypted endpoints are disconnected	
Encrypt When Possible	Connected encrypted - Endpoints with encryption capabilities. Connected non-encrypted - endpoints without encryption capabilities	Connected only if encrypted. Non-encrypted endpoints are disconnected.	

^{*} System Flag =

FORCE ENCRYPTION FOR UNDEFINED PARTICIPANT IN WHEN AVAILABLE MODE

Moving from the Entry Queue to Conferences or Between Conferences

Participants can be moved from the Entry Queue and the destination conference if both conferencing entities have the same Profile settings, i.e. from SVC Only Entry Queue to SVC Only conference and from mixed CP and SVC Entry Queue to a mixed CP and SVC conference, etc.

When moving participants from the Entry Queue to the destination conference, or when the Collaboration Server user moves AVC participants from one conference to another (SVC participants cannot be moved between conferences), the connection rules are similar and they are summarized in the table below:

Moving Participants from the Entry Queue to the Destination conference or between conferences Based on the Encryption Settings

Destination	Current Participant Encryption Status			
Conference	Encrypted		Non-Encrypted	
Encryption Setting	*Flag = NO	*Flag = YES	*Flag = NO	*Flag = YES
No Encryption	Move succeeds, connected encrypted		Move succeeds, connected non-encrypted	
Encrypt All	Move succeeds, connected encrypted.		Move fails, disconnected.	
Encrypt When Possible	Move succeeds, connected encrypted	Move succeeds, connected encrypted	Move succeeds, connected non-encrypted	Connected only if endpoint was a defined participant in the source conference. Otherwise, move fails.

^{*} System Flag =

FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE

Recording Link Encryption

Recording Links are treated as regular participants, however the

ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF system flag must be set to **YES** if a non-encrypted Recording Link is to be allowed to connect to an encrypted conference.

The following table summarizes the connection possibilities for a Recording Link that is to be connected to a conference for each of the conference profile and Entry Queue encryption options.

Connections by Recording Link and Conference Encryption Settings

Conference Profile Setting	Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_ LINK_IN_ENCRYPT_CONF			
Frome Setting	YES	NO		
Encrypt All	Connected encrypted if possible, otherwise connected non-encrypted.	Connected only if encrypted, otherwise disconnected		
No Encryption	Connected non-encrypted	Connected non-encrypted		
Encrypt when possible	Connected encrypted if possible, otherwise connected non-encrypted.	Connected encrypted if possible, otherwise connected non-encrypted.		

Enabling Media Encryption for a Conference

Media encryption is enabled at three levels:

- MCU level Setting the Encryption Flags
- Conference level Enabling Encryption in the Profile
- Participant level Enabling Encryption at the Participant Level

You must first set the system flags for the MCU before media encryption can be enabled for the conference and participants.

Setting the Encryption Flags

Enabling the media encryption for the MCU is usually performed once an it is applicable to all conferences running on the MCU.

To modify the Encryption flags:

- 1 Click Setup>System Configuration.
 - The **System Flags** dialog box opens.
- 2 Set the
 - FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_AVAILABLE_MODE flag to YES or NO.
- 3 If recording will be used in encrypted conferences, set the ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF flag to YES or NO.
- 4 Click OK.

For more information, see Modifying System Flags.

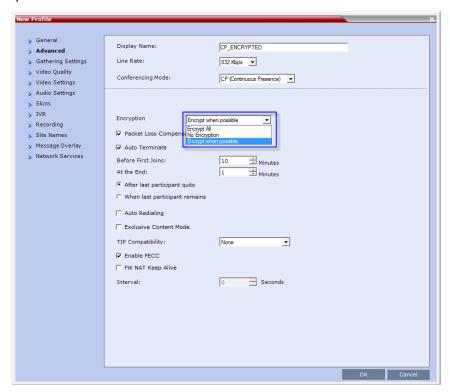
5 Reset the MCU for flag changes to take effect.

Enabling Encryption in the Profile

Encryption for the conference is in the Profile and cannot be changed once the conference is running.

To enable encryption at the conference level:

» In the Conference Profile Properties – Advanced dialog box, select one of the following Encryption options:



- Encrypt All Encryption is enabled for the conference and all conference participants must be encrypted.
- > No Encryption Encryption is disabled for the conference.
- Encrypt when possible enables the negotiation between the MCU and the endpoints and let the MCU connect the participants according to their capabilities, where encryption is the preferred setting. For connection guidelines see Mixing Encrypted and Non-encrypted Endpoints in one Conference.

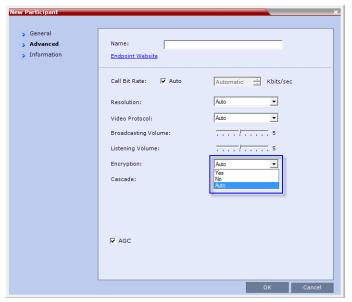
For more information about recording encrypted conferences, see Recording Link Encryption.

Enabling Encryption at the Participant Level

You can select the encryption mode for each of the defined participants. Encryption options are affected by the settings of the flag in the system configuration. Undefined participants are connected with the Participant Encryption option set to **Auto**, inheriting the conference/Entry Queue encryption setting.

To enable encryption at the participant level:

» In the Participant Properties – Advanced dialog box, in the Encryption list, select one of the following options: Auto, On, or Off.

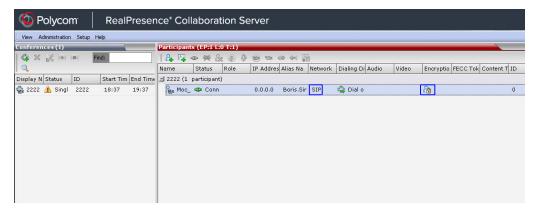


- > **Auto** The participant inherits the conference/Entry Queue encryption setting. The participant connects as encrypted only if the conference is defined as encrypted.
- > Yes The participant joins the conference/Entry Queue as encrypted.
- > No The participant joins the conference/Entry Queue as non-encrypted.

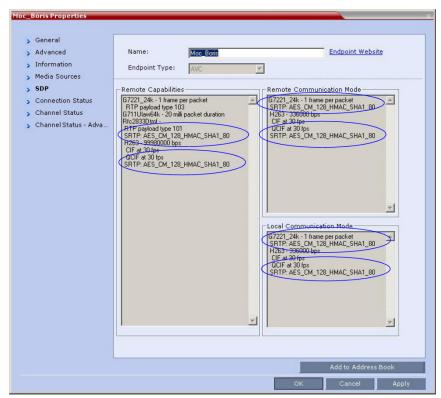
Monitoring the Encryption Status

The conference encryption status is indicated in the Conference Properties - General dialog box.

The participant encryption status is indicated by a check mark in the **Encryption** column in the **Participants** list pane.



The participant encryption status is also indicated in the **Participant Properties – SDP** tab, where SRTP indication is listed for each encrypted channel (for example, audio and video).



An encrypted participant who is unable to join a conference is disconnected from the conference. The disconnection cause is displayed in the **Participant Properties – Connection Status** dialog box, Security Failure indication, and the Cause box identifies the encryption related situation.

For more information about monitoring, see Conference and Participant Monitoring.

Setting Conferences for Telepresence Mode (AVC CP)

Collaboration Server supports the Telepresence Mode in AVC CP conferences allowing multiple participants to join a telepresence conference from RPX and OTX high definition rooms as well as traditional, standard definition video conferencing systems.

OTX (Telepresence) and RPX (RealPresence) room systems are configured with high definition cameras and displays that are set up to ensure that all participants share a sense of being in the same room.

Participants using two RealPresence RPX HD 400 Room Systems



The following are examples of situations where an Collaboration Server is needed for Telepresence configurations:

- RPX to OTX
- RPX 2-cameras/screens to RPX 4-cameras/screens
- 3 or more RPXs
- 3 or more OTXs

Collaboration Server Telepresence Mode Guidelines

System Level

- The Collaboration Server system must be licensed for Telepresence Mode.
- The system must be activated with a **Telepresence enabled** license key.

Conference Level

- The Telepresence Mode and Telepresence Layout Mode fields are only displayed in the Conference Profile dialog box if the Collaboration Server has a Telepresence license installed.
- A Telepresence conference must have **Telepresence Mode** enabled in its profile.
- In Telepresence Mode, ITP sites are automatically detected.
- When Telepresence Mode is selected in a conference profile, the following options are disabled:
 - Borders
 - > Site Names
 - Speaker Indication
 - > Skins
 - Same Layout
 - Presentation Mode
 - Auto Layout
 - Lecture Mode
- The master (center) camera is used for video, audio and content.
- Conference Templates can be used to simplify the setting up Telepresence conferences where
 precise participant layout and video forcing settings are crucial. Conference Templates:
 - > Save the conference Profile.
 - > Save all participant parameters including their Personal Layout and Video Forcing settings.
- An ongoing Telepresence conference can be saved to a Conference Template for later re-use. For more information see Conference Templates.

Automatic Detection of Immersive Telepresence (ITP) Sites

When the conference **Telepresence Mode** is set to **Auto** (Default) ITP endpoints are automatically detected.

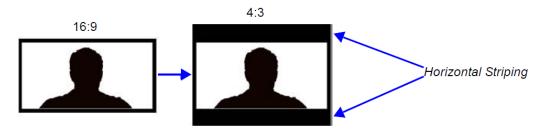
If an ITP endpoint is detected in such conference, ITP features are applied to **all** endpoints and the Collaboration Server sends conference video with the following options disabled:

- Borders
- Site names
- Speaker indication
- Skins
- Same Layout
- Presentation Mode
- Auto Layout
- Lecture Mode

The ITP features are dynamic, and if all ITP endpoints disconnect from the conference, normal conference video is resumed for the remaining all participants. ITP features are re-applied to all participants should an ITP endpoint re-connects to that conference.

Horizontal Striping

Horizontal Striping is used by the Collaboration Server in order to prevent cropping and preserve the aspect ratio of video for all Telepresence Modes.

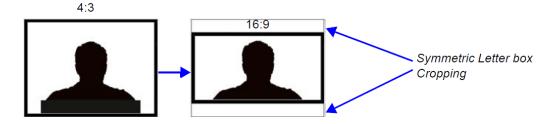


Cropping

Cropping is used by the Collaboration Server in order to preserve the aspect ratio of video for all Telepresence Modes.

Cropping is controlled by the **ITP_CROPPING** system flag in the system configuration, providing different cropping options according to the endpoints participating in the Telepresence conference.

By default, the flag is set to **ITP**. In this mode, the area to be stripped is cropped equally from the top and the bottom (as shown in the example below). For more details, see Modifying System Flags.



Gathering Phase with ITP Room Systems

When a conference is configured to include a Gathering Phase, only one endpoint name is displayed for the ITP room in the connected participant list of the Gathering slide. The ITP room endpoint with the suffix 1 in its name receives the Gathering slide.

Aspect ratio for standard endpoints

Standard endpoints (non-ITP) receive video from the Collaboration Server with the same aspect ratio as that which they transmitted to the Collaboration Server.

Skins and Frames

When Telepresence Mode is enabled, no Skin is displayed and the system uses a black background. Frames around individual layout windows and the speaker indication are disabled.

RPX and OTX Video Layouts

Additional video layouts have been created to give Telepresence operators more video layout options when configuring OTX and RPX room systems. These additional video layout options are available to all endpoints on both conference layout and Personal Layout levels.

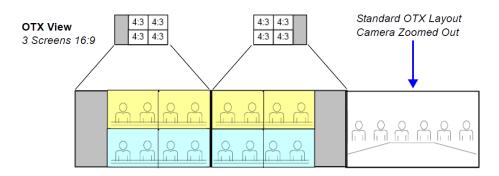
OTX / RPX - Additional Video Layouts

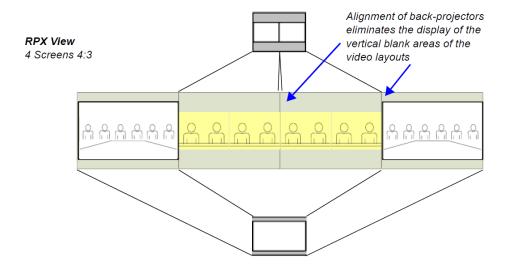
Number of Endpoints	Layouts
1	
2	4:3 4:3
3	4:3 4:3 4:3 4:3 4:3 4:3
4	4:3 4:3 4:3 4:3 4:3 4:3 4:3 4:3 4:3 4:3 4:3 4:3
5	
9	
10+	

The following example illustrates the use of standard and additional Collaboration Server Telepresence layouts when connecting four Room Systems as follows:

- Two OTX Room Systems
 - 2 active cameras
 - > 6 screens
- Two RPX Room Systems
 - > 8 cameras
 - > 8 screens

RPX and OTX Room System connected using the RealPresence Collaboration Server





Room Switch Telepresence Layouts

The Room Switch Telepresence layouts normally controlled by the MLA can be managed by the MCU to speed updating the conference layouts in large conferences with many endpoints.

Whether the MLA or the MCU controls the Room Switch Telepresence layouts is determined by the **MANAGE_TELEPRESENCE_ROOM_SWITCH_LAYOUTS** flag. This flag must be manually added before changing its value. No system reset is required.

The values are:

- NO (Default) The MCU does not manage Telepresence Room Switch Layouts and they continue to be managed by the MLA.
- YES The MCU manages Telepresence Room Switch Layouts.

When the MCU controls the Telepresence Room Switch layouts (MANAGE_TELEPRESENCE_ROOM_SWITCH_LAYOUTS = YES) the display is affected according to the Telepresence Mode Settings in the Conference Profile as follows:

- If the Telepresence Mode = ON
 - ➤ If no ITP endpoints are connected to the conference, the RMX Room Switch layout applies, in which case only the speaker is seen.
 - When a single participant using an ITP endpoint with either single or multiple screens connects to the conference, the participant will see black screens.
- If the Telepresence Mode = AUTO
 - If no ITP endpoints are connected to the conference, the RMX CP layout applies (unless the conference layout is defined).
 - > When a single participant using an ITP endpoint with multiple screens connects to the conference, the participant will see black screens.
 - When a single participant using an ITP endpoint with a single screen connects to the conference, the MCU will display a self-view of the participant.
- When a TIP system with 3 screens joins a conference, the layout is updated on all screen simultaneously.
- When a Polycom ITP system with 2, 3, or 4 screens joins the conference, the layout is updated on all screens simultaneously.

Telepresence Display Decision Matrix

How the speaker video is displayed on the screens of the conference participants is dependent on the relationship between the number of screens the speaker endpoint contains and the number of screens of the endpoints of the other conference participants.

The following Telepresence Display Decision Matrix table below indicates how the speaker video will be displayed on the various participant endpoints, when the MCU is managing Telepresence Room Switch conference layouts.

Number of Screens		Speaker Endpoint				
		1	2	3	4	
Participant Endpoint	1	Speaker EP: 1 Displaying EP (mirror): 1 EP1	Speaker EP: 2 1 Displaying EP (mirror): 2 1 EP1	Speaker EP: 2 1 3 Displaying EP (mirror): 2 1 3 EP1	Speaker EP: 4 2 1 3 Displaying EP (mirror): 4 2 1 3 EP1	
	2	Speaker EP: 1 Displaying EP (mirror): 1 EP-2 EP1	Speaker EP: 2 1 Displaying EP (mirror): 2 1 EP2 EP1	Speaker EP: 2 1 3 Displaying EP (mirror): 2 1 3 EP2 EP1	Speaker EP: 4 2 1 3 Displaying EP (mirror): 4 2 1 3 EP2 EP1	
Partic	3	Speaker EP: 1 Displaying EP (mirror): EP2 EP1 EP3	Speaker EP: 2 1 Displaying EP (mirror): 2 1 EP2 EP1 EP3	Speaker EP: 2 1 3 Displaying EP (mirror): 2 1 3 EP2 EP1 EP3	Speaker EP: 4 2 1 3 Displaying EP (mirror): 4 2 1 3 EP2 EP1 EP3	
	-4	Speaker EP: 1 Displaying EP (mirror): 1 EP4 EP2 EP1 EP3	Speaker EP: 2 1 Displaying EP (mirror): 2 1 EP4 EP2 EP1 EP3	Speaker EP: 2 1 3 Displaying EP (mirror): 2 1 3 EP4 EP2 EP1 EP3	Speaker EP: 4	

For example, if the speaker's endpoints has two screens and the participant's endpoint only one, the participant's display is divided into two video layout cells with each video layout cell showing the input of one of the speaker's screens (endpoint).

If the participant endpoint has two screens, and the speaker endpoint only one, the speaker's video will be displayed on one of the participant's screens, while the second screen remains black.

Guidelines for Managing the Room Switch Telepresence Layouts by the MCU

- Only Room Switch layouts can be managed by the MCU. CP (Continuous Presence) layouts continue to be managed by the MLA.
- Only CP-AVC conferences are supported.
- Lync Clients (with CSS add-in) are supported.
- SVC endpoints are not supported.
- It is recommended that the Speaker Change Threshold be set to 3 seconds.
- Telepresence endpoints are named using a text name followed by a number. For example, if an OTX Telepresence room is named Oak, the three endpoint names would be Oak1, Oak2, and Oak3.
- Lecture mode is not supported in Telepresence Room Switch conferences managed by the MCU.
 (This is because in Lecture mode, unlike Room Switch mode, the lecturer receives the CP layout of conference participants.)
- Personal layouts are disabled. Therefore, any features that use personal layouts like Click&View can not be used to change the layout, and Click&View DTMF digits will be ignored.

- Changing the flag affects only future conferences. Conferences currently running are not affected.
- The Send Content To Legacy Endpoints feature is enabled by default when Telepresence mode is enabled.
- Layout attributes (no skins, no site names and no borders) should continue for Telepresence layouts managed by the RMX.

Sending Content to Legacy Endpoints in Telepresence Conferences

The Collaboration Server can be configured to manage the layouts of to H.323/SIP/ISDN endpoints that do not support H.239 Content (legacy endpoints) over the video (people) channel in Telepresence conferences when Content is being sent. This feature is controlled using the

FORCE_LEGACY_EP_CONTENT_LAYOUT_ON_TELEPRESENCE flag. This flag must be added to change the value.

The values of the flag are:

- NO (Default) The MCU does not manage the layouts while Content is sent. Personal layout changes, for example, by MLA, override the default MCU layout. Legacy endpoints may not display Content in Telepresence conferences due to layout changes.
- **YES** The MCU manages the layouts while *Content* is sent. Personal layout changes, for example, by MLA, are ignored. The layouts for legacy endpoints are managed by the MCU.

Guidelines for Sending Content to Legacy Endpoints in Telepresence Conferences

- MLA layout change requests for legacy endpoints will be ignored until Content is stopped. At that point, MLA can be used again.
- Click&View can not be used to change the layout while Content is being sent.
- The Polycom Touch Control can not be used to change the layout while Content is being sent.

Content Display on Legacy Endpoints in Telepresence Conferences

When Content is sent to legacy endpoints in Telepresence conferences, their video layout automatically changes to the Content layout which is defined by the system flag

LEGACY_EP_CONTENT_DEFAULT_LAYOUT. If MLA is managing the Telepresnce layout prior to Content being sent, the MCU takes over managing the layout of Legacy endpoints once Content is started. The video layouts of the other conference participants continue to be managed by MLA.

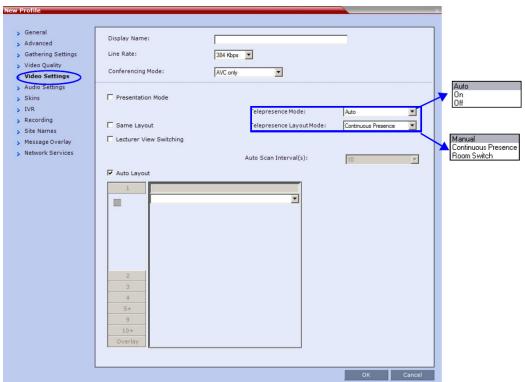
If MLA was managing the Telepresence layouts, when Content ends, control of the layouts for legacy endpoints goes back to the MLA after a short time.

Enabling Telepresence Mode

Telepresence Mode must be configured in a new or existing Conference Profile.

To enable Telepresence in a new or existing Conference Profile:

- 1 In the RMX Management pane, click Conference Profiles.
- 2 Click the **New Profiles** button or open an existing Conference Profile.
- 3 Define the various profile **General**, **Advanced**, **Gathering Settings** and **Video Quality** parameters. For more information on defining Profiles, see Defining New Profiles.
- 4 Click the Video Settings tab.



- 5 In the **Telepresence Mode** field, select one of the following options:
 - > **OFF** When OFF is selected, normal conference video is sent by the Collaboration Server.
 - ➤ AUTO (Default) The ITP features are dynamic. When AUTO is selected and an ITP endpoint is detected, ITP features are applied to the conference video for all participants. If all ITP endpoints disconnect from the conference, normal conference video is resumed for all remaining participants. ITP features are re-applied for all participants should an ITP endpoint re-connect to the conference.
 - When Telepresence Mode is set to **Auto** and a one-screen Telepresence unit is in use, the Collaboration Server controls layouts instead of the *MLA*. For more information see *Polycom Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions*.
 - ON ITP features are always applied to the conference video for all participants regardless of whether there are ITP endpoints connected or not.

6 In the **Telepresence Layout Mode** field, select the Telepresence Layout Mode to be used in the conference. This field is used by VNOC operators and Polycom Multi Layout Applications to retrieve Telepresence Layout Mode information from the Collaboration Server.

The following modes can be selected (as required by the VNOC and Polycom Multi Layout Applications):

- > Manual
- > Continuous presence Room Continuous Presence (Default)
- > Room Switch Voice Activated Room Switching
- 7 Select the required video layout.
- 8 Click OK.

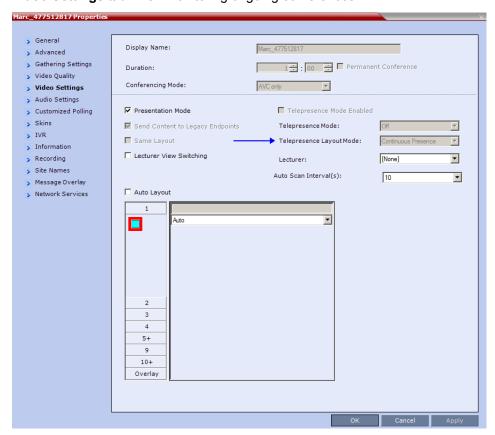


When **Telepresence Mode** is enabled, the **Skins** options are disabled as the system uses a black background and the frames and speaker indication are disabled.

Monitoring Telepresence Mode

Monitoring Ongoing Conferences

An additional status indicator, **Telepresence Mode Enabled**, is displayed in the **Conference Properties - Video Settings** tab when monitoring ongoing conferences.



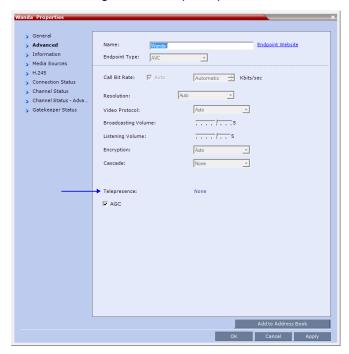


The **Telepresence Mode Enabled**, **Telepresence Mode** and **Telepresence Layout Mode** fields are only enabled if the Collaboration Server has a Telepresence license installed.

If Telepresence Mode is enabled, a check mark is displayed in the check box. This option is grayed as this is a status indicator and cannot be used to enable or disable Telepresence Mode.

Monitoring Participant Properties

An additional status indicator, **Telepresence**, is displayed in the **Participant Properties - Advanced** tab when monitoring conference participants.



The Telepresence mode of the participant is indicated:

- **RPX** the participant's endpoint is transmitting 4:3 video format.
- **OTX** the participant's endpoint is transmitting 16:9 video format.
- None.

Creating Multiple Cascade Links Between Telepresence Conferences

You can create multiple Cascading links between Collaboration Servers hosting conferences that include Immersive Telepresence Rooms (ITP) such as Polycom's OTX and RPX Room Systems.

Guidelines for Creating Multiple Cascading Links between Conferences

- Basic Cascading topology is used. For more information see the RealPresence Collaboration Server 800s Administrator's Guide, Basic Cascading using IP Cascaded Link.
- Multiple Cascade Links between conferences are implemented by creating a Link Participant which
 consists of a main link and sub-links which are automatically generated and sequentially numbered.
 For more information see Creating a Link Participant, Creating a Link Participant.
- All cascaded links must use H.323 protocol.
- Multiple Cascade Links are supported in CP conferencing mode.
- The number of cascading links is defined manually according to the maximum number of Room System cameras in the cascaded conference.
- When the active speaker is in an Immersive Telepresence Room, Multiple Cascade Links are used, one link for each of the Room System's cameras.
 - > An RPX 4xx Room System requires 4 Cascaded Links to carry the video of its 4 cameras.
 - > An RPX 2xx Room System requires 2 Cascaded Links to carry the video of its 2 cameras.
 - An OTX 3xx Room System requires 3 Cascaded Links to carry the video of its 3 cameras. The OTX Room System must be configured as Room Switch in order to send multiple streams. When configured in CP Mode, its cameras zoom out and all 3 screens are sent as one stream.
- The number of links is defined when creating the Link Participant. Each conference in the cascade
 must have a Link Participant with the same number of Multiple Cascade Links defined. Calls from
 Link Participants not defined with the same number of links are rejected. Number of cascading links
 is not identical for all conferences is listed as the Call Disconnection Cause. For more information see
 Creating a Link Participant and Monitoring Multiple Cascade Links.
- Although it is possible to disconnect and reconnect specific Multiple Cascade Links using the RealPresence Collaboration Server Web Client / RealPresence Collaboration Server Manager it not advisable to do so.
 - > If the main link is disconnected all sub-links are disconnected and deleted.
 - Reconnecting the main link reconnects all sub-links.
 - > If a sub-link is disconnected it remains disconnected until it is manually reconnected.
 - ➤ The number of Multiple Cascade Links cannot be modified while any of the links are in a disconnected state. All previous links must be deleted before modification is possible.
 - For more information see Monitoring Multiple Cascade Links.
- A Link Participant can be dragged from the address book into a conference.
 - ➤ If it is the first Link Participant in the conference, the number of Multiple Cascade Links defined for the participant are created and connected.
 - ➤ If it is not the first Link Participant in the conference, the number of Multiple Cascade Links defined for the participant is ignored.

- If there are insufficient resources to connect all Multiple Cascade Links in either of the RMXs, none
 of the links are connected and resources deficiency -0 is listed as the Call Disconnection Cause. For
 more information see Monitoring Multiple Cascade Links.
- Multiple Cascade Links that are not used by MLA are inactive but continue to consume resources.
- All RMXs participating in the cascade must have the same Telepresence Mode definitions, either all defined as CP or all defined as Room Switch.
- When Multiple Cascade Links are defined in the Conference Profile, the Layout Type field of the Link Participant's Participant Properties - Media Sources dialog box is set to Conference and cannot be modified.
- TIP Telepresence Rooms (CTS) are supported without Content. For more information see the Collaboration With Cisco's Telepresence Interoperability Protocol (TIP).

Enabling and Using Multiple Cascade Links

The settings required to enable Multiple Cascade Links on the RMX are minimal and are described in Creating a Link Participant.

Most of the layout configuration is performed using Polycom's Multipoint Layout Application (MLA).

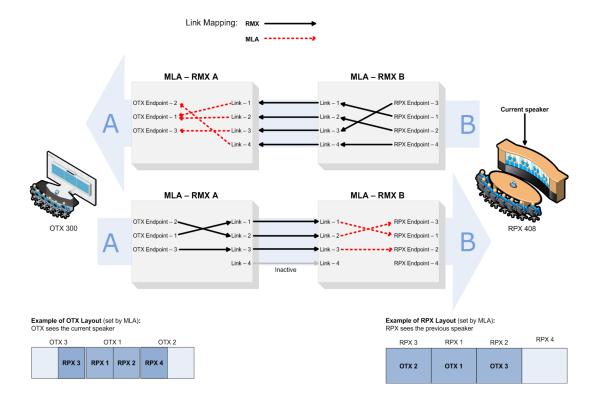
The figures RMX Telepresence Layout Mode - Room Switch and RMX Telepresence Layout Mode - Continuous Presence show example layouts and media flows when MLA is configured for a cascading conference between two RMXs.

In the figure RMX Telepresence Layout Mode - Room Switch:

- The OTX Room System connects to RMX A.
- The RPX Room System connects to RMX B.
- This layout requires that the Telepresence Layout Mode to be set to Room Switch in the Conference Profiles of the Cascading Conferences in each RMX.
- The current speaker is a participant in the RPX ITP Room.

Directional media flows, A ≒ B, are shown separately for readability purposes.

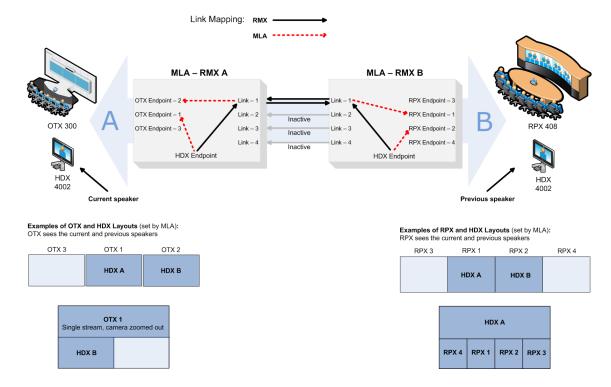
RMX Telepresence Layout Mode - Room Switch



In the RMX Telepresence Layout Mode - Continuous Presence figure:

- > An HDX endpoint and an OTX Room System connects to RMX A.
- An HDX endpoint and an RPX Room System connects to RMX B.
- ➤ This layout requires that the **Telepresence Layout Mode** to be set to **Continuous Presence** in the Conference Profiles of the Cascading Conferences in each RMX.
- > The current speaker is the HDX endpoint connected to RMX A.

RMX Telepresence Layout Mode - Continuous Presence



For more information see:

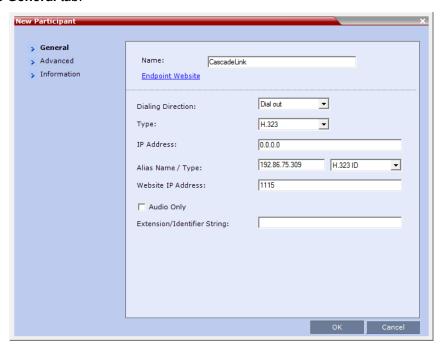
- Telepresence Layout Mode.
- Polycom® Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions.
- Polycom® Immersive Telepresence (ITP) Deployment Guide

Creating a Link Participant

Link Participant in the Dial Out RMX

The Link Participant is defined in the **New Participant** dialog box.

In the General tab:



- Dialing Direction must be selected as Dial out.
- Type must be selected as H.323.

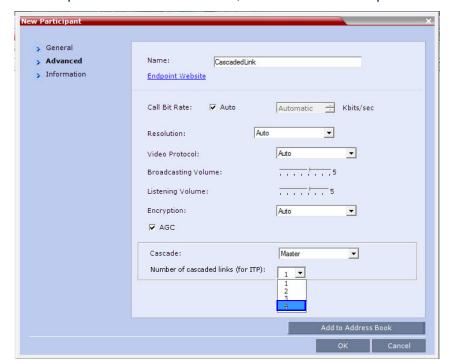
For more information see the Creating a Cascade Enabled Dial-out/Dial-in Participant Link.

In the Advanced tab:

(This field is only enabled if the RMX system is licensed for Telepresence Mode.)

- In the Cascade drop-down menu, select either Master or Slave.
- In the Number of cascaded links (for ITP) drop-down menu, select the maximum number of Multiple Cascade Links required according to the number of Room System endpoints in the cascaded conference.

This field enables the administrator to select the maximum number of Multiple Cascade Links required according to the number of Room System endpoints in the cascaded conference.



For example if an RPX 4xx is included, the number of links required is 4.

The RMX automatically adds a number suffix to the name of the **Link Participant**, for example if the **Participant Link Name** is **CascadeLink** and the **Number of cascaded links (for ITP)** field is set to **4**, the following **Multiple Cascade Links** are created:

- CascadeLink-1
- CascadeLink-2
- CascadeLink-3
- CascadeLink-4

Participant Link in the Dial In RMX

The call from Participant Link defined in the Dial-out RMX is identified by the Dial-in RMX as having been initiated by a Participant Link.

Suffixes are appended to the Multiple Cascade Links according to the **Number of cascaded links** (for ITP) field depending on whether the Dial -In Participant Link is defined or un-defined:

Participant Link is un-defined

The Multiple Cascade Link names are automatically assigned by the RMX.

For example on a RMX 1500 the names of the links are:

- POLYCOM RMX 1500-1
- POLYCOM RMX 1500-2
- POLYCOM RMX 1500-3, etc.

Participant Link is a defined

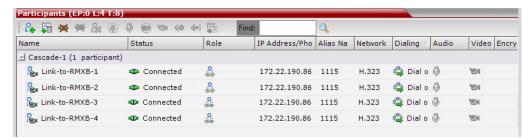
The Multiple Cascade Link names are assigned according to the name of the defined participant that is to function as the cascade link and the Number of cascaded links (for ITP) information sent by the calling Dial-Out Participant Link.

For example if the defined participant that is to function as the cascade link is named Cascade_Link_From_B the names of the links are:

- Cascade_Link_From_B-1
- Cascade_Link_From_B-2
- Cascade_Link_From_B-3, etc.

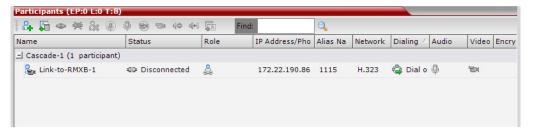
Monitoring Multiple Cascade Links

Multiple Cascade Links connections can be monitored in the Participants list of the RMX Web Client / RMX Manager main screen:

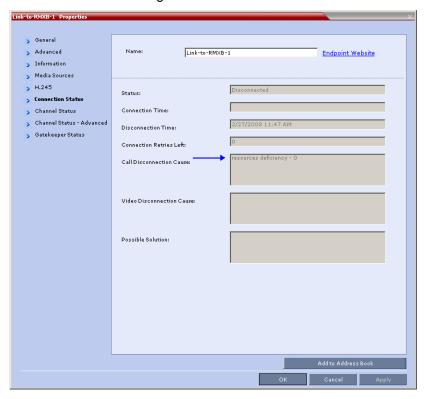


Disconnection Causes

- If there are insufficient resources to connect all the required links:
 - None of the links are connected.
 - The first link is listed as Disconnected in the Participants list of the RMX Web Client / RMX Manager main screen.



 Resource deficiency is listed as the Call Disconnection Cause in the Participant Properties -Connection Status dialog box.



- If a calling Link Participant is not defined with same number of links as all the other Link Participants in the cascaded conferences:
 - The call is rejected.
 - > The Call Disconnection Cause is: Number of cascading links is not identical for all conferences.

Additional Conferencing Information

Various conferencing modes and video features require additional settings, such as system flag settings, conference parameters and other settings. In depth explanations of these additional settings are described in the following sections:

- Video Preview (AVC Participants Only)
- Auto Scan and Customized Polling in Video Layout (CP Conferences Only)
- Packet Loss Compensation (LPR and DBA) AVC CP Conferences
- Network Quality Indication (AVC Endpoints)
- Lecture Mode (AVC CP Only)
- Audio Algorithm Support
- Automatic Muting of Noisy Endpoints (AVC Endpoints)

Video Preview (AVC Participants Only)



Video Preview is not supported when the Collaboration Server is in Ultra Secure Mode. For more information see Ultra Secure Mode.

Collaboration Server users can preview the video sent from the participant to the conference (MCU) and the video sent from the conference to the participant. It enables the Collaboration Server users to monitor the quality of the video sent and received by the participant and identify possible quality degradation.

The video preview is displayed in a separate window independent to the Collaboration Server Web Client. All Web Client functionality is enabled and conference and participant monitoring as well as all other user actions can be performed while the video preview window is open and active. Live video is shown in the preview window as long as the window is open. The preview window closes automatically when the conference ends or when participant disconnects from the conference. It can also be closed manually by the Collaboration Server user.

Video Preview Guidelines

- Video Preview is supported in CP Conferencing Mode only.
- Video preview is available for AVC participants. It is not available for SVC participants.
- Video preview window size and resolution are adjusted to the resolution of the PC that displays the preview.
- Video Preview of the video sent from the conference to the participant is shown according to the line
 rate and video parameters of the level threshold to which the participant is connected.

- In versions up to and including Version 7.2.2, only users with Administrator authorization could request to view a video preview. In later versions, all users can view a video preview.
- Only one preview window can be displayed for each Collaboration Server Web Client connection (workstation).
- Only one preview window can be displayed for a single conference and up to four preview windows
 can be displayed for each media card on different workstations (one per workstation and one per
 conference). For example, if the Collaboration Server contains two media cards, and there are 5
 conferences running on the Collaboration Server, if five conferences are running on the same media
 card, only four conferences can be previewed from four different workstations. If four or less
 conferences are running on one media card and the remaining conferences are running on the other
 media card, all five conferences can be previewed.
- Live video that is shown in the preview window does not include the Content when it is sent by the participant.
- Video Preview is supported in cascaded conferences.
- If the video preview window is opened when the IVR slide is displayed to the participant, it will also be displayed in the video preview window.
- Video Preview is supported with H.264 High Profile.
- Video Preview is not supported for endpoints using the RTV protocol.
- Video Preview is disabled in encrypted conferences.
- Video preview cannot be displayed when the participant's video is suspended.
- Participant's video preview and the Polycom Desktop application (such as CMAD) window cannot be
 open and running simultaneously on the same PC as both require the same DirectDraw resource.

Workstation Requirements to Display Video Preview

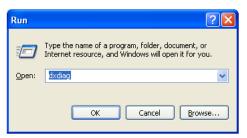
To be able to display the video preview window, the following minimum requirements must be met:

- Windows XP. Windows Vista and Windows 7
- Internet Explorer 7 and later
- DirectX is installed
- DirectDraw Acceleration must be enabled and no other application is using the video resource
- Hardware acceleration must be enabled

Testing your Workstation

To ensure that your workstation can display the video preview window:

- 1 In Windows, click Start > Run.
 - The **Run** dialog box opens.
- 2 In the Open field, type dxdiag, and press Enter or click OK.



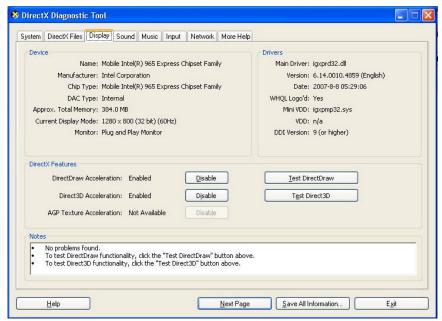
A confirmation message is displayed.

3 Click Yes to run the diagnostics.

The **DirectX Diagnostic Tool** dialog box opens.

4 Click the Display tab.

To be able to display the video preview window, the **DirectDraw Acceleration** and **Direct3D Acceleration** options must be **Enabled**.



If the video card installed in the PC does not support DirectDraw Acceleration, a black window may be viewed in the Video Preview window.

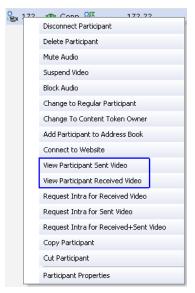
5 Click the Exit button.

Previewing the Participant Video

You can preview the video sent from the participant to the conference (MCU) and the video sent from the conference to the participant by selecting the appropriate option from the Participant's pop-up menu.

To preview the participant video:

- 1 List the conference participants in the Participants pane.
- 2 Right-click the participant whose video you want to preview and then click one of the following options:



- View Participant Sent Video To display the video sent from the participant to the conference.
- View Participant Received Video To display the video sent from the conference to the participant.

The Video Preview window opens.





If the video card installed in the PC does not support DirectDraw Acceleration, a black window may be viewed.

Auto Scan and Customized Polling in Video Layout (CP Conferences Only)

Auto Scan enables you to define a single cell in the conference layout to cycle the display of participants that are not in the conference layout.

Customized Polling allows the cyclic display to be set to a predefined order for a predefined time period. The cyclic display only occurs when the number of participants is larger than the number of cells in the layout.

Guidelines for Using Auto Scan and Customized Polling

- Auto Scan and Customized Polling are supported in AVC CP conferences only.
- Participants that are in the conference layout will not appear in the Auto Scan enabled cell.
- If Customized Polling is not used to define the order of the Auto Scan it will proceed according to order in which the participants connected to the conference.
- If the user changes the conference layout, the Auto Scan settings are not exported to the new layout.
 If the user changes the conference layout back to the layout in which Auto Scan was enabled, Auto Scan with the previous settings will be resumed.

Enabling the Auto Scan and Customized Polling (CP Only Conferences)

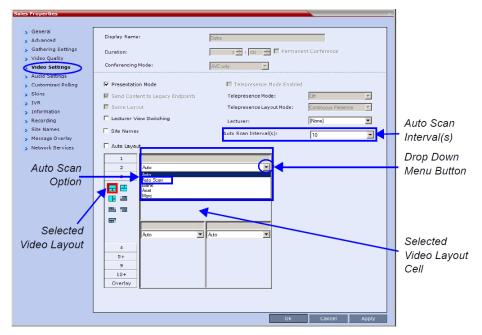
Auto Scan and Customized Polling are enabled during the ongoing conference, in the **Conference Properties - Video Settings** dialog box.

Enabling the Auto Scan

You enable the Auto Scan feature by selecting it in the Video Layout cell.

To enable Auto Scan:

- 1 In the Collaboration Server Web Client Main Screen Conference list pane, double-click the conference or right-click the conference and then click **Conference Properties**.
- 2 In the Conference Properties General dialog box, click Video Settings.
 The Video Settings dialog box is displayed.



3 If Auto Layout check box is selected, clear it.

- 4 In the video layout cell to be designated for Auto Scan, click the drop-down menu button and select **Auto Scan**.
- 5 Select from the **Auto Scan Interval(s)** list the scanning interval in seconds.
- 6 Click the **Apply** button to confirm and keep the dialog box open, or Click **OK**.

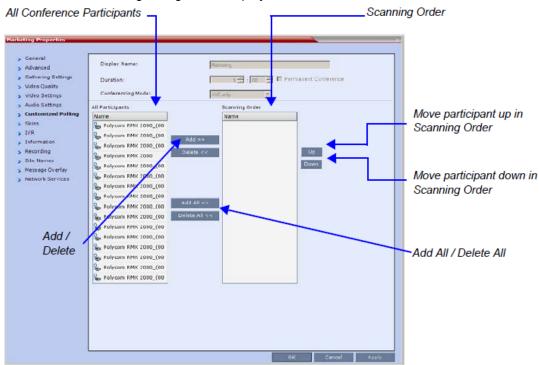
Customized Polling

The order in which the Auto Scanned participants are displayed in the Auto Scan enabled cell of the video layout can be customized.

To define the scanning order in the Customized Polling tab:

- 1 Open the Conference Properties dialog box.
- 2 Click the Customized Polling tab.

The Customized Polling dialog box is displayed.



All conference participants are listed in the left pane (**All Participants**) while the participants that are to be displayed in the Auto Scan enabled cell of the video layout are listed in the right pane (**Scanning Order**).

The dialog box buttons are summarized in the following table:

Customized Polling Dialog Box Command Buttons

Button	Description
Add	Select a participant and click this button to <i>Add</i> a the participant to the list of participants to be Auto Scanned. The participants name is removed from the All Participants pane.
	The participants name is removed from the All Participants pane.
Delete	Select a participant and click this button to Delete the participant from the list of participants to be Auto Scanned.
	The participants name is moved back to the All Participants pane.
Add All	Add all participants to the list of participants to be Auto Scanned.
	All participants' names are removed from the All Participants pane.
Delete All	Delete all participant from the list of participants to be Auto Scanned.
	All participants' names are moved back to the All Participants pane.
Up	Select a participant and click this button to move the participant Up in the Scanning Order.
Down	Select a participant and click this button to move the participant Down in the Scanning Order.

3 Click the **Apply** button to confirm and keep the dialog box open, or click **OK**.

Packet Loss Compensation (LPR and DBA) AVC CP Conferences

Lost Packet Recovery (LPR) and Dynamic Bandwidth Allocation (DBA) help minimize media quality degradation that can result from packet loss in the network. Packet loss Compensation is available in AVC CP Conferencing Mode only and is not supported in SVC Conferencing Mode or CP and SVC Conferencing Mode.

Packet Loss

Packet Loss refers to the failure of data packets, transmitted over an IP network, to arrive at their destination. Packet Loss is described as a percentage of the total packets transmitted.

Causes of Packet Loss

Network congestion within a LAN or WAN, faulty or incorrectly configured network equipment or faulty cabling are among the many causes of Packet Loss.

Effects of Packet Loss on Conferences

Packet Loss affects the quality of:

- Video frozen images, decreased frame rate, flickering, tiling, distortion, smearing, loss of lip sync
- Audio drop-outs, chirping, audio distortion

Content – frozen images, blurring, distortion, slow screen refresh rate

Lost Packet Recovery

The Lost Packet Recovery (LPR) algorithm uses Forward Error Correction (FEC) to create additional packets that contain recovery information. These additional packets are used to reconstruct packets that are lost, for whatever reason, during transmission. Dynamic Bandwidth Allocation (DBA) is used to allocate the bandwidth needed to transmit the additional packets.

Lost Packet Recovery Guidelines

- If packet loss is detected in the packet transmissions of either the video or Content streams:
 - LPR is applied to both the video and Content streams.
 - > DBA allocates bandwidth from the video stream for the insertion of additional packets containing recovery information.
- LPR is supported in H.323 and SIP networking environments only.
- In LPR-enabled Continuous Presence conferences:
 - > Both LPR-enabled and non-LPR-enabled endpoints are supported.
 - ➤ The LPR process is not applied to packet transmissions from non-LPR-enabled IP (H.323 and SIP) and ISDN (Collaboration Server 1500/2000/4000) endpoints.
 - Non-LPR-enabled endpoints can be moved to LPR-enabled conferences.
 - > LPR-enabled endpoints cannot be moved to non-LPR-enabled conferences.
- In LPR-enabled Video Switched conferences (Collaboration Server 1500/2000/4000):
 - ➤ H.323 and SIP endpoints are supported.
 - ➤ When cascading between conferences running on Collaboration Server and MGC (Polycom legacy MCU), LPR is not supported over the link between the two conferences.
 - Non-H.323 participants cannot be created, added or moved to LPR-enabled Video Switched conferences.
- When connecting via an Entry Queue:
 - ➤ A participant using an LPR-enabled endpoint can be moved to a non-LPR-enabled conference. The participant is connected with LPR enabled.
 - SIP and ISDN/PSTN (Collaboration Server 1500/2000/4000) participants cannot be moved to LPR-enabled Video Switched conferences.

Enabling Lost Packet Recovery

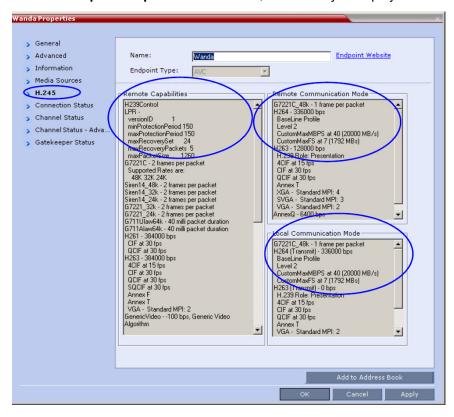
LPR is enabled or disabled in the Conference Profile dialog box.

- CP Conferences LPR is enabled by default in the New Profile Advanced dialog box.
- VSW Conferences If Video Switching is selected, the LPR check box is automatically cleared and LPR is disabled. LPR can be enabled for VSW conferences but H.320 and SIP participants will not be able to connect.

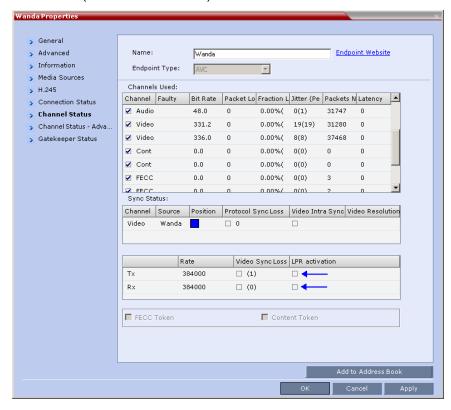
For more information, see Defining New Profiles.

Monitoring Lost Packet Recovery

In the Participant Properties - H.245 tab, LPR activity is displayed in all three panes.

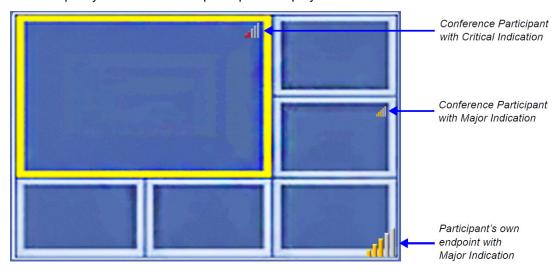


In the **Participant Properties – Channel Status** tab, check box indicators show LPR activation in the local and remote (transmit and receive) channels.



Network Quality Indication (AVC Endpoints)

If network quality issues occur, the **Network Quality** icon provide information to participants about their own network quality and that of other participants displayed in the cells of the conference Video Layout.



Network Quality Levels

Network quality is determined by the percentage of packet loss according to the following default threshold values:

- Packet loss less than 1% is considered Normal
- Packet loss in the range of 1% 5% is considered Major
- Packet loss above 5% is considered Critical.

Major and Critical states are indicated with yellow and red indicator bars respectively.



When network quality improves from Critical to Major remaining stable for 5 seconds, the Network Quality Indicator is changed accordingly and when network quality improves from Major to Normal, remaining stable for 5 seconds, the Network Quality Indicator is no longer displayed.

Indication Threshold Values

The default Major and Critical indication threshold values can be modified by manually adding the following System Flags and modifying their values as required.

Network Quality Icon - Indication Threshold Flags

Flag	Description
NETWORK_IND_MAJOR_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from Normal to Major . Default: 1
NETWORK_IND_CRITICAL_PERCENTAGE	The percentage degradation due to packet loss required to change the indicator from Major to Critical . Default: 5

For more information see Manually Adding and Deleting System Flags.

Guidelines for Displaying the Network Quality icons

Network Quality icons are not supported in SVC Conferencing Mode and AVC - Video switched conferences (Collaboration Server 1500/2000/4000).

Network Quality icons are displayed for:

- The video channel only in AVC Conferencing Mode.
 Content, audio and FECC channel quality issues are not indicated.
- The participant's own endpoint:
 - > Network Quality icons are displayed by default and can be disabled
 - > For media transmitted to and received from the Collaboration Server (Video in / Video out).
- Participants displayed in the cells of the conference video layout:
 - Network Quality icons are not displayed by default and can be enabled
 - > The media transmitted from the endpoint to the Collaboration Server (Video in).

Customizing Network Quality Icon Display

Display of the Network Quality icon can be customized for the participant's own endpoint or for the Participants displayed in the cells of the conference Video Layout.

The display of Network Quality icon (showing or hiding the icon) and the position of the icon in the video layout cell can be customized by manually adding the following System Flags and modifying their values as required.

Network Quality Icon - Display Customization Flags

Flag	Description
DISABLE_SELF_NETWORK_IND	Disable the display of the Network Quality icon of the participant's own endpoint.
	Default: NO
	Range: YES / NO

Network Quality Icon - Display Customization Flags

Flag	Description	
DISABLE_CELLS_NETWORK_IND	Disable the display of Network Quality icons displayed in the cells of the conference Video Layout. Default: YES Range: YES / NO	
SELF_IND_LOCATION	Change the location of the display of the Network Quality icon of the participant's own endpoint. Default: BOTTOM_RIGHT Range: TOP_LEFT TOP TOP_RIGHT BOTTOM_LEFT BOTTOM BOTTOM_RIGHT	
CELL_IND_LOCATION	Change the location of the display of Network Quality icon displayed in the cells of the conference Video Layout. Default: TOP_RIGHT Range: BOTTOM_LEFT BOTTOM_RIGHT TOP_LEFT TOP_RIGHT	

For more information see the Manually Adding and Deleting System Flags.

Lecture Mode (AVC CP Only)

Lecture Mode enables all participants to view the lecturer in full screen while the conference lecturer sees all the other conference participants in the selected layout while he/she is speaking. When the number of sites/endpoints exceeds the number of video windows in the layout, switching between participants occurs every 15 seconds. Conference participants cannot change their Personal Layouts while Lecture Mode is enabled.

Automatic switching is suspended when one of the participants begins talking, and it is resumed automatically when the lecturer resumes talking.

Lecture Mode is available only in AVC CP Conferencing Mode.

Enabling Lecture Mode

Lecture Mode is enabled at the conference level by selecting the lecturer. Conference participants cannot change their Personal Layouts while Lecture Mode is enabled.

Automatic switching between participants viewed on the lecturer's screen is enabled in the conference Profile.

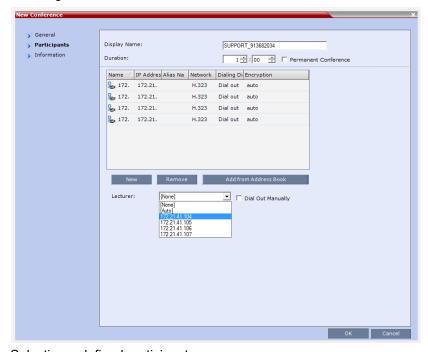
Selecting the Conference Lecturer

Selecting a lecturer for the ongoing conference, enables the Lecture Mode. You can select the lecturer:

- during the definition of the ongoing conference
- after the conference has started and the participants have connected to the conference.

To select the lecturer and enable the Lecture Mode while starting the conference:

 In the Conference Properties - Participant dialog box, enable the Lecture Mode in one of the following methods:



Selecting a defined participant:

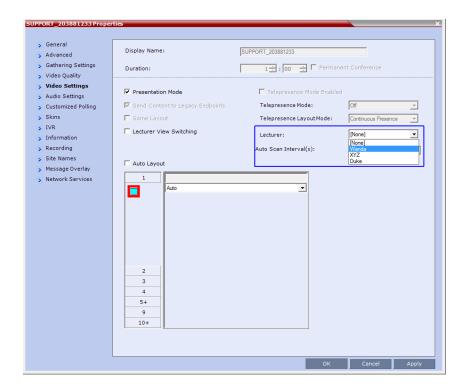
- a Add participants to the conference either from the Address book or by defining new participants.
- **b** In the **Lecturer** field, select the lecturer from the list of the defined participants.

To automatically select the lecturer, in the **Lecturer** field, select [Auto].

In this mode, the conference speaker becomes the lecturer.

To select the lecturer and enable the Lecture Mode during the ongoing conference:

- 1 Make sure that the participant you want to designate as the lecturer has connected to the conference.
- 2 In the Conference Properties Video Settings dialog box, in the Lecturer field, select the lecturer from the list of the connected participants.

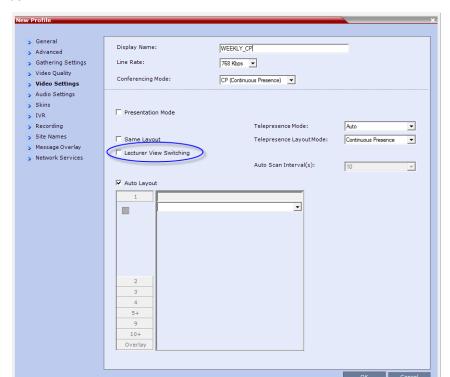




Defined dial out participants and dial in participants are considered to be two separate participants even if they have the same IP address/number. Therefore, if a defined dial-out participant is added to the conference and the same participant then dials in (before the system dialed out to that participant) the system creates a second participant in the Participants list and tries to call the dial-out participant. If the dial-out participant was designated as the conference lecturer, the system will not be able to replace that participant with the dial-in participant that is connected to the conference.

Enabling the Automatic Switching

Automatic switching between participants viewed on the lecturer's screen is enabled in the conference Profile, or during the ongoing conference, in the Conference Properties.



 In the Profile Properties - Video Settings dialog box, select the Lecturer View Switching check box.

This option is activated when the conference includes more sites than windows in the selected layout. If this option is disabled, the participants will be displayed in the selected video layout without switching.

For more information about Profile definition, see Defining AVC-Based Conference Profiles.

 Once the conference is running, in the Conference Properties - Video Settings dialog box, select the Lecturer View Switching check box.

Lecture Mode Monitoring

A conference in which the Lecture Mode is enabled is started as any other conference. The conference runs as an audio activated Continuous Presence conference until the lecturer connects to the conference. The selected video layout is the one that is activated when the conference starts. Once the lecturer is connected, the conference switches to the Lecture Mode.

When **Lecturer View Switching** is activated, it enables automatic switching between the conference participants in the lecturer's video window. The switching in this mode is not determined by voice activation and is initiated when the number of participants exceeds the number of windows in the selected video layout. In this case, when the switching is performed, the system refreshes the display and replaces the last active speaker with the current speaker.

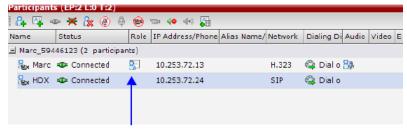
When one of the participants is talking, the automatic switching is suspended, showing the current speaker, and it is resumed when the lecturer resumes talking.

If the lecturer is disconnected during an Ongoing Conference, the conference resumes standard conferencing.

Forcing is enabled at the Conference level only. It applies only to the video layout viewed by the lecturer as all the other conference participants see only the lecturer in full screen.

If an asymmetrical video layout is selected for the lecturer (i.e. 3+1, 4+1, 8+1), each video window contains a different participant (i.e. one cannot be forced to a large frame and to a small frame simultaneously).

When Lecture Mode is enabled for the conference, the lecturer is indicated by an icon in the **Role** column of the **Participants** list.



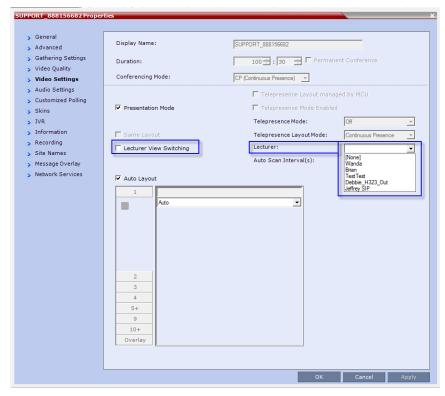
Participant designated as the Lecturer

To control the Lecture Mode during an Ongoing Conference:

During the Ongoing Conference, in the Conference Properties - Video Settings dialog box you can:

- Enable or disable the Lecture Mode and designate the conference lecturer in the Lecturer list; select
 None to disable the Lecture Mode or select a participant to become the lecturer to enable it.
- Designate a new lecturer.

 Enable or disable the Lecturer View Switching between participants displayed on the lecturer monitor by selecting or clearing the Lecturer View Switching check box.



• Change the video layout for the lecturer by selecting another video layout.

Restricting Content Broadcast to Lecturer

Content broadcasting can be restricted to the conference lecturer only, when one of the conference participants is set as the lecturer (and not automatically selected by the system). Restricting the Content Broadcast prevents the accidental interruption or termination of H.239 Content that is being shared in a conference.

Content Broadcast restriction is enabled by setting the

RESTRICT_CONTENT_BROADCAST_TO_LECTURER system flag to **ON**. When set to **OFF** (default) it enables all users to send Content.

When enabled, the following rules apply:

- Content can only be sent by the designated lecturer. When any other participant tries to send Content, the request is rejected.
- If the Collaboration Server user changes the designated lecturer (in the Conference Properties -Video Settings dialog box), the Content of the current lecturer is stopped immediately and cannot be renewed.
- The Collaboration Server User can abort the H.239 Session of the lecturer.
- Content Broadcasting is not implemented in conferences that do not include a designated lecturer and the lecturer is automatically selected by the system (for example, in Presentation Mode).

Muting Participants Except the Lecturer (AVC CP Only)

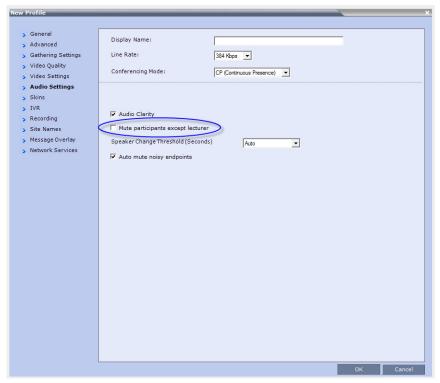
When the **Mute Participants Except Lecturer** option in the Conference Profile is enabled, the audio of all participants in the conference except for the lecturer can be automatically muted upon connection to the conference. This prevents other conference participants from accidentally interrupting the lecture, or from a noisy participant affecting the audio quality of the entire conference. Muted participants cannot unmute themselves unless they are unmuted from the Collaboration Server Web Client/RMX Manager.

Guidelines for Muting all the Participants Except the Lecturer

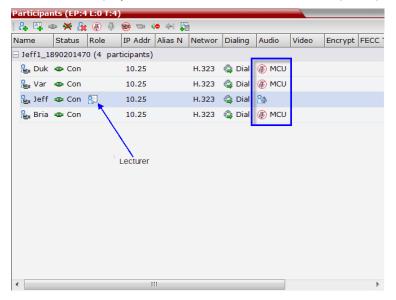
- Both administrators and operators (users) are allowed to set the Mute Participants Except Lecturer
 option.
- When the Mute Participants Except Lecturer option is enabled, the mute indicator on the participant
 endpoints are not visible because the mute participants was initiated by the MCU. Therefore, it is
 recommended to inform the participants that their audio is muted by using the Message Overlay
 functions.
- When the Mute Participants Except Lecturer option is enabled in the Conference Profile settings, all conferences to which this profile is assigned will start with this option enabled. All participants, except for the designated lecturer, are muted.
- The Mute Participants Except Lecturer option can be enabled or disabled at any time after the start
 of the conference. When enabled, it allows all the conference participants to converse before the
 lecturer joins the conference or before they are muted. When disabled, it unmutes all the participants
 in the conference.
- If the endpoint of the designated lecturer is muted when the lecturer connects to the conference, the lecturer remains muted until the endpoint has been unmuted.
- When you replace a lecturer, the MCU automatically mutes the previous lecturer and unmutes the new lecturer.
- When you disconnect a lecturer from the conference or the lecturer leaves the conference, all participants remain muted but are able to view participants in regular video layout until the you disable the Mute Participants Except Lecturer option.
- A participant can override the Mute Participants Except Lecturer option by activating the Mute All Except Me option using the appropriate DTMF code, provided the participant has authorization for this operation in the IVR Services properties. The lecturer audio is muted and the participant audio is unmuted. You can reactivate the Mute Participants Except Lecturer option after a participant has previously activated the Mute All Except Me option. The participant is muted and the lecturer, if designated, is unmuted.
- In cascaded conferences, all participants (including the link participants) except the lecturer are muted. Only the lecturer is not muted.

Enabling the Mute Participants Except Lecturer Option

The Mute Participants Except Lecturer option is enabled or disabled (default) in the Conference Profile or in an ongoing conference in the **Profile Properties - Audio Settings** tab.



When the Mute Participants Except Lecturer option is enabled and a conference has started, the **Mute by MCU** icon is displayed in the Audio column in the Participants pane of each participant that is muted.



Audio Algorithm Support

The Collaboration Server supports the following audio algorithms in AVC conferences: G.711, G.722, G.722.1, G.722.1C, G.729A, G.719 (Collaboration Server 1500/2000/4000), G. 728, G.723.1 Polycom Siren 7 (in mono), Siren14, Siren 22 (in mono or stereo) and SirenLPR.

Polycom's proprietary Siren 22 and industry standard G.719 audio algorithms are is supported for participants connecting with Polycom endpoints.

The Siren 22 audio algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications. Siren 22 requires less computing power and has much lower latency than alternative wideband audio technologies.

The SirenLPR audio algorithm provides CD-quality audio for better clarity and less listener fatigue with audio and visual communication applications.

In SVC conferences, the system supports SAC (Scalable Audio Coding) audio algorithm.

Audio Algorithm Support Guidelines

- Siren 22 and G.719 are supported in both mono and stereo.
- Stereo is supported in H.323 calls only.
- Siren 22 is supported by Polycom HDX and Group series endpoints, version 2.0 and later.
- G.728 is supported in H.323, SIP and ISDN (Collaboration Server 1500/2000/4000) environments.
- SirenLPR is enabled by default and can be disabled by setting the system flag ENABLE_SIRENLPR, to NO.
- SirenLPR is supported:
 - In IP (H.323, SIP) calls only.
 - ➤ In CP and VSW (Collaboration Server 1500/2000/4000) conferences.
 - ➤ With Polycom CMAD and HDX 3.0.1 and later and Group series endpoints.
 - For mono audio at audio line rates of 32Kbps, 48Kbps and 64Kbps.
 - For stereo audio at audio line rates of 64Kbps, 96Kbps and 128Kbps.

SIP Encryption

The **ENABLE_SIRENLPR_SIP_ENCRYPTION** System Flag enables the SirenLPR audio algorithm when using encryption with the SIP protocol.

The default value of this flag is **NO** meaning SirenLPR is disabled by default for SIP participants in an encrypted conference. To enable SirenLPR the System Flag must be added to **system.cfg** and its value set to **YES**.

Mono

The Siren 22, G.719 and SirenLPR mono audio algorithms are supported at the following bit rates

Siren22, G.719 and SirenLPR Mono vs Bitrate

Audio Algorithm	Minimum Bitrate (kbps)
Siren22 64k	
Siren22 48K	
Siren22_32k	
G.719_64k	384
G.719_48k	
G.719_32k	
G.728 16K	
G.719_64k	384
SirenLPR_48k	256
Siren22_48K	
G.719_48k	
G.7221C_48k	
Siren14_48k	
SirenLPR_32k	
Siren22_32k	
G.719_32k	128
G.7221C_32k	
Siren14_32k	
SirenLPR	64
SirenLPR	48
SirenLPR	32

Stereo

The Siren 22Stereo, G.719Stereo and SirenLPR audio algorithms are supported at the following bit rates.

Siren22Stereo, G.719Stereo and SirenLPR vs Bitrate

Audio Algorithm	Minimum Bitrate (kbps)	
Siren22Stereo_128k		
SirenLPRStereo_128k	1024	
G.719Stereo_128k		

Siren22Stereo, G.719Stereo and SirenLPR vs Bitrate

Audio Algorithm	Minimum Bitrate (kbps)	
Siren22Stereo_96k		
SirenLPRStereo_96k	E40	
G.719Stero_96k	512	
Siren14Stero_96k		
SirenLPRStereo_64k		
G.719Stereo_64k	384	
Siren22Stereo_64k	304	
Siren14Stereo_64k		

Audio algorithms supported for ISDN (Collaboration Server 1500/2000/4000 only)

Supported Audio Algorithm vs Bitrate

Audio Algorithm	Minimum Bitrate (kbps)
G.722.1C 48K	
G.722.1C 32K	
G.722.1C 24K	
Siren14 48K	256
Siren14 32K	250
Siren14 24K	
G.722.1 32K	
G.722.1 24K	
G.722.1 16K	
G.722 48K	
G.722 56K	
G.722 64K	256
G.711 56K	
G.711 64K	
G.728 16K	

Supported Audio Algorithm vs Bitrate

Audio Algorithm	Minimum Bitrate (kbps)	
G.722.1C 32K		
G.722.1C 24K		
Siren14 32K		
Siren14 24K		
G.722.1 32K		
G.722.1 24K	128	
G.722 48K	120	
G.722 56K		
G.722 64K		
G.711 56K		
G.711 64K		
G.728 16K		
G.722.1 16K		
G.722.1C 24K		
Siren14 24K		
G.722 48K		
G.722 56K	96	
G.722 64K		
G.711 56K		
G.711 64K		
G.728 16K		
G.728 16K	64	

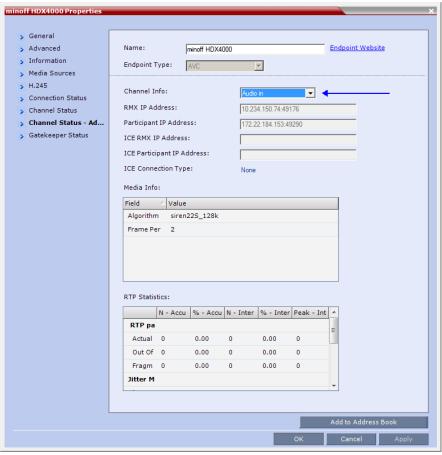
Monitoring Participant Audio Properties

The audio algorithm used by the participant's endpoint can be verified in the **Participant Properties - Channel Status** dialog box.

To view the participant's properties during a conference:

- 1 In the Participants list, right click the desired participant and select Participant Properties.
- 2 Click the Channel Status Advanced tab.
 The Participant Properties Channel Status Advanced dialog box is displayed.

3 In the Channel Info field, select Audio In or Audio Out to display the audio parameters.



4 Click the **OK** button.

Automatic Muting of Noisy Endpoints (AVC Endpoints)



This feature is not supported in the RMX 1800.

The Collaboration Server can detect AVC-enabled endpoints with a noisy audio channel and automatically mute them, reducing the noise heard by other conference participants. When the auto muted endpoint becomes the speaker the endpoint is automatically un-muted by the system. If the speaker halts his/her conversation and the line still emits noises, the endpoint will be automatically muted again.

When the endpoints are automatically muted by the MCU, no indication is displayed in the Collaboration Server Web Client or RMX Manager as the system does not consider it as a deliberate mute.

Automatic muting of noisy AVC endpoints is enabled only when the following conditions are met:

- The **Auto mute noisy endpoints** check box in the **Profile Properties Audio Settings** dialog box is selected (default in CP conferences).
- The ENABLE_SELECTIVE_MIXING flag is set to YES (default).

If one of these settings is disabled, the automatic muting of noisy endpoints is disabled.

Guidelines for Automatically Muting Noisy Endpoints

The automatic muting of noisy AVC-enabled endpoints can be used according to the following guidelines:

- Automatic muting of noisy AVC endpoints is available on Polycom RealPresence Collaboration Server (RMX) 1500/2000/4000 with MPMx cards only.
- The Auto mute noisy endpoints check box in the Profile Properties Audio Settings dialog box is enabled only when the ENABLE_SELECTIVE_MIXING flag is set to YES (default).
- It affects only AVC-based and audio only endpoints (non-SAC endpoints)
- It does not affect SVC-based endpoints
- It is supported in CP conferences and in Mixed CP and SVC conferences.
- In a mixed CP and SVC conferences, only the AVC-based endpoints can be automatically muted. If the noisy endpoint is SVC-based, its audio channel will not be sent to the AVC-based endpoints, but it will be sent to the other SVC-based endpoints.
- MCU reset is not required when changing the ENABLE_SELECTIVE_MIXING flag setting.
- When upgrading from a version prior to 8.1, the Auto mute noisy endpoints option is not automatically
 enabled in the existing Profiles and it has to be manually enabled, if required.
 - In new Profiles that are created after the upgrade, the **Auto mute noisy endpoints** option is automatically enabled.
- If your conferencing environment includes the Polycom DMA, the conferences that are started from
 the DMA will not include the *Auto mute noisy endpoints* parameter as it is not part of the DMA Profiles.
 In such a case, when the parameter setting is unknown, the system will enable or disable the
 automatic muting of noisy endpoints according to the flag setting if the flag is set to YES, it will be
 enabled in the conference.

The following table summarizes the state (enabled or disabled) of the Automatic muting of noisy endpoints feature depending on the ENABLE_SELECTIVE_MIXING flag setting and the **Auto mute noisy endpoints** setting in the **Profile Properties - Audio Settings**:

Conditions for enabling/disabling the automatic muting of noisy endpoints

ENABLE_SELECTIVE_MIXING flag Setting	Auto mute noisy endpoints setting	Automatic muting of noisy endpoints State
YES	Yes (check box selected)	Enabled
YES	No (check box cleared)	Disabled
YES	Unknown (for example, the conference is started from the DMA)	Enabled
NO	Yes (check box selected)	Disabled
NO	No (check box cleared)	Disabled
NO	Unknown (for example, the conference is started from the DMA)	Disabled

Enabling or Disabling the Automatic Muting of Noisy Endpoints

The automatic muting of noisy endpoints can be enabled or disabled at the conference level (in the Conference Profile) or at the system level, by changing the **ENABLE_SELECTIVE_MIXING** flag setting.

In new MCU installations, the automatic muting of noisy endpoints is automatically enabled on the MCU as the **ENABLE_SELECTIVE_MIXING** flag is set to **YES** and the **Auto mute noisy endpoints** check box in the *Profile Properties - Audio Settings* tab is selected.

You can disable the automatic muting of noisy endpoints by either setting the system flag to NO or clearing the **Auto mute noisy endpoints** check box in the **Profile Properties - Audio Settings** tab.

If required, it is recommended to disabled the automatic muting of noisy endpoints at the conference level, in the conference Profile without changing the flag settings.

In existing MCU sites, following the software upgrade the automatic muting of noisy endpoints is disabled at the conference level in the existing conference Profile and has to be manually enabled in these profiles. This option is automatically enabled when creating a new Profile.

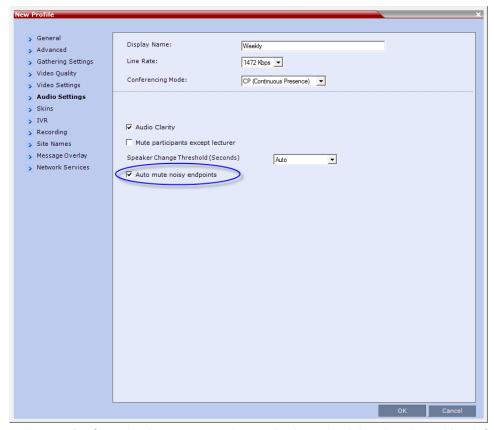
Enabling or Disabling the Automatic Muting of Noisy Endpoints at the Conference Level

If the **ENABLE_SELECTIVE_MIXING** flag is set to YES, the automatic muting of noisy endpoints can be enabled or disabled at the conference level in the **Conference Profile - Audio Settings** dialog box.

If the **ENABLE_SELECTIVE_MIXING** flag is set to NO, the automatic muting of noisy endpoints is disabled at the conference level and cannot be enabled in the **Conference Profile - Audio Settings** dialog box.

To disable/enable the automatic muting of noisy endpoints in the Conference Profile:

1 In a new or existing Conference Profile, click the **Audio Settings** tab.



- In new Profiles, the Auto mute noisy endpoints check box is selected by default.
- In existing profiles (after software upgrade from a version prior to 8.1), the Auto mute noisy endpoints check box is cleared.
- 2 To enable the automatic muting of noisy endpoints, click the Auto mute noisy endpoints check box.
- 3 Click OK.

Enabling or Disabling the Automatic Muting of Noisy Endpoints at the MCU Level

You can disable the automatic muting of noisy endpoints at the MCU level by changing the **ENABLE_SELECTIVE_MIXING** flag setting to **NO**.

In such a case, the automatic muting of noisy endpoints at the conference level (in the **Conference Profile** - **Audio Settings** dialog box) is disabled.

To modify the system flag setting:

 To modify NABLE_SELECTIVE_MIXING flag setting to NO, manually add it to system.cfg file and set its value to NO.

For more details, see the Modifying System Flags.

Permanent Conference

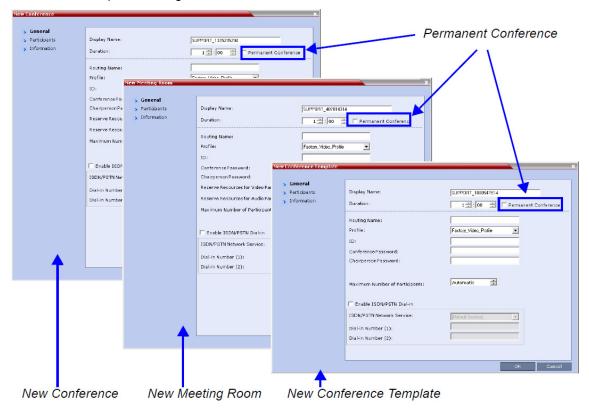
A Permanent Conference is any ongoing conference with no pre-determined End Time continuing until it is terminated by an administrator, operator or chairperson.

Guidelines

- Resources are reserved for a Permanent Conference only when the conference has become ongoing.
- Resources are allocated to a Permanent Conference according to the Reserve Resources for Video Participants field. If the number of defined dial-out participants exceeds the value of this field, the Collaboration Server automatically replaces the number in the Reserve Resources for Video Participants field with the number of defined dial-out participants in the Permanent Conference.
- Auto Terminate is disabled in Permanent Conferences.
- If participants disconnect from the Permanent Conference, resources that were reserved for its video and audio participants are released.
- Entry Queues, Conference Reservations and SIP Factories cannot be defined as Permanent Conferences.
- Additional participants can connect to the conference, or be added by the operator, if sufficient resources are available.
- The maximum size of the Call Detail Record (CDR) for a Permanent Conference is 1MB.

Enabling a Permanent Conference

The Permanent Conference option is selected in the New Conference, New Meeting Room or New Conference Templates dialog boxes.



Closed Captions (AVC Endpoints)



This option is not supported with Collaboration Server 1800.

Endpoints can provide real-time text transcriptions or language translations of the video conference by displaying captions. The captions for a conference may be provided by the captioner who is present in the conference, or the captioner may use a telephone or web browser to listen to the conference audio. When the captioner sends a unit of text, all conference participants see it on the main monitor for 15 seconds. The text then disappears automatically.

The captioner may enter caption text using one of the following methods:

- Remotely, via a dial-up connection to the system's serial RS-232 port.
- In the room using equipment connected directly to the serial port.
- In the room or remotely, using the Polycom HDX web interface.

Closed Captions Guidelines

- The captions display properties are configured on the endpoint sending the captions.
- Closed Captions content is defined from the endpoint. The Collaboration Server only transmits it to the endpoints.
- When enabled, captions are available to all endpoints supporting FECC.
- Captions are supported in H.323 and SIP connections.
- The FECC indications during ongoing conferences are used when sending captions.
- When Closed Captions option is enabled for the MCU, muting an endpoint may cause the display of the Far Mute indication on all the screens of the endpoints connected to the conference.
- The Closed Captions option is not supported in cascading conferences (captions they can only be viewed in the local conference) as FECC is not supported in cascading links.
- Site name display is not affected by captions display.
- Captions are supported by the Collaboration Server in the following configurations and conferencing modes:
 - MPMx Card Configuration Modes.
 - CP Conferencing Mode.
 - Encrypted and non-encrypted conferences.
 - Conferences with content sharing.

Enabling Closed Captions

Captions are enabled by a system flag. By default, Closed Captions are disabled.

To change the flag value:

- 1 On the Collaboration Server menu, click **Setup > System Configuration**.
 - The **System Flags** dialog box opens.
- 2 In the MCMS_PARAMETERS tab, click the New Flag button.
 - The **New Flag** dialog box is displayed.
- 3 In the New Flag field enter ENABLE_CLOSED_CAPTION.
- 4 In the Value field enter YES to enable or NO to disable Closed Captions display.
- 5 Click **OK** to close the **New Flag** dialog box.
 - The new flag is added to the flags list.
- 6 Click **OK** to close the **System Flags** dialog box.



For flag changes (including deletion) to take effect, reset the MCU. For more information, see Resetting the Collaboration Server.

Defining Cascading Conferences



Cascading information applies to AVC Conferencing Mode (CP and mixed CP and SVC) only. Cascading is not supported with SVC Conferencing Mode.

Cascading enables administrators to connect one conference directly to one or several conferences, depending on the topology, creating one large conference. The conferences can run on the same MCU or different MCUs.

There are many reasons for cascading conferences, the most common are:

- Connecting two conferences on different MCUs at different sites.
- Utilizing the connection abilities of different MCUs, for example, different communication protocols, such as, serial connections and ISDN, etc.

Conferences are Cascaded when a link is created between two conferences, usually running on two different MCUs.

Cascading Link Properties

Cascade links are treated as endpoints in CP conferences. They are allocated resources as any other endpoint according to Default Minimum Threshold Line Rates and Resource Usage Summary.

They transmit audio, video and content between conferences as well as DTMF codes input from other endpoints in the conference.

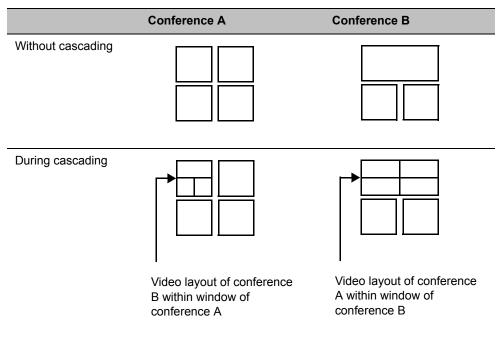
Setting the Video Layout in Cascading conferences require additional consideration.

Setting the Video Layout in Cascading conferences (CP and mixed CP and SVC)

When cascading two conferences, the video layout displayed in the cascaded conference is determined by the selected layout in each of the two conferences. Each of the two conferences will inherit the video layout of the other conference in one of their windows.

In order to avoid cluttering in the cascaded window, it is advised to select appropriate video layouts in each conference before cascading them.

Video Layouts in Cascaded Conferences



Guidelines for Setting the Video Layout in Cascading Conferences

To ensure that conferences can be cascaded and video can be viewed in all conferences the following guidelines are recommended:

- The same version installed on all MCUs participating the cascading topology
- The same license installed on all MCUs participating the cascading topology
- Same Conference Parameters are defined in the Profile of the conferences participating in the cascading topology
 - Conference line rates should be identical
 - > Content rate should be identical
 - Same encryption settings
- DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences
- DTMF forwarding is suppressed
- The video layout of the link is set to 1x1 by the appropriate system flag.
- Cascaded links in 1x1 video layout are in SD resolution.
- When the Mute Participants Except Lecturer option is enabled in the Conference Profile, all
 participants (including the link participants) except the lecturer are muted. Only the lecturer is not
 muted.
- Gathering is not supported in Cascading Conferences.

Flags Controlling Cascading Layouts

- Setting the FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION System Flag to YES (default) automatically forces the cascading link to Full Screen (1x1) in CP conferences, hence displaying the speaker of one conference to a full window in the video layout of the other conference.
 - Set this flag to **NO** when cascading between an Collaboration Server and an MCU that is functioning as a Gateway, if the participant layouts on the MCU are not to be forced to 1X1.
- Setting the AVOID_VIDEO_LOOP_BACK_IN_CASCADE System Flag to YES (default) prevents
 the speaker's image from being sent back through the participant link from the cascaded conference.
 This can occur in cascaded conferences with conference layouts other than 1x1. It results in the
 speaker's own video image being displayed in the speaker's video layout.

This option is supported with:

- ➤ In IP (H.323, SIP) and ISDN environments.
- Basic Cascading of Continuous Presence and Video Switched conferences. If a Master MCU has two slave MCUs, participants connected to the slave MCUs will not receive video from each other.
- Video resolution will be according to the Resolution Configuration, or VSW profile.

For more details on defining system flags, see Modifying System Flags.

DTMF Forwarding

When two conferences are connected over an IP link, DTMF codes from one conference are not forwarded to the second conference with the exception of the following operations that are available throughout the conference and the forwarding of their DTMF codes is not suppressed (i.e. they will apply to both conferences):

- Terminate conference.
- Mute all but me.
- Unmute all but me.
- Secure conference.
- Unsecure conference.



During cascading between a gateway and a conference **all** DTMF codes are forwarded from the gateway to the conference and vice versa.

Play Tone Upon Cascading Link Connection

The Collaboration Server can be configured to play a tone when a cascading link between conferences is established. The tone is played in both conferences.

This tone is not played when the cascading link disconnects from the conferences.

The tone used to notify that the cascading link connection has been established cannot be customized.

The option to play a tone when the cascading link is established is enabled by setting the System Flag CASCADE_LINK_PLAY_TONE_ON_CONNECTION to YES.

Default value: NO.

The tone volume is controlled by the same flag as the IVR messages and tones: IVR_MESSAGE_VOLUME.

Possible Cascading Topologies

The following cascading topologies are available for setting cascading conferences:

- Basic Cascading only two conferences are connected (usually running on two different Collaboration Servers). The cascaded MCUs reside on the same network.
- Star Cascading one or several conferences are connected to one master conference. Conferences are usually running on separate MCUs. The cascaded MCUs reside on the same network.
- MIH (Multi-Hierarchy) Cascading several conferences are connected to each other in Master-Slave relationship. The cascaded MCUs can reside on different networks.

System configuration and feature availability change according to the selected cascading topology.



For properly share content in cascaded conferences, predefined dial in and out link participants must be defined with Master/Slave settings in the conferences.

When Cascading between the Collaboration Server and third party MCUs, the participant defined in the Collaboration Server conference must be defined as Master.

When cascading between the Collaboration Server and a Codian MCU, set the system flag **ENABLE_CODIAN_CASCADE** to **YES** to ensure that the Collaboration Server is defined as a Master in cascading conferences at all times.

Basic Cascading

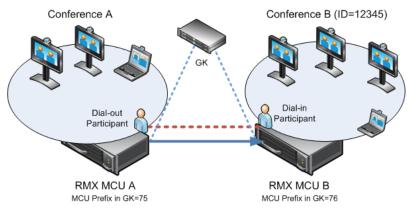
In this topology, a link is created between two conferences, usually running on two different MCUs. The MCUs are usually installed at different locations (states/countries) to save long distance charges by connecting each participant to their local MCU, while only the link between the two conferences is billed as long distance call.

- In Collaboration Server 1500/2000/4000, this is the only topology that enables both IP and ISDN cascading links. ISDN is not supported with Collaboration Server 1800.
- When linking two conferences using an IP cascading link:
 - > The destination MCU can be indicated by:
 - ♦ IP address
 - ♦ H.323 Alias
 - > Both MCUs must be located in the same network.
- With Collaboration Server 1500/2000/4000, one MCU can be used as a gateway.
- The configuration can include two Collaboration Servers or one Collaboration Server and one MGC.
- Multiple Cascade Links enabling Cascading between RMXs hosting conferences that include Immersive Telepresence Rooms (ITP) such as Polycom's OTX and RPX Room Systems can be defined. For more information see Creating Multiple Cascade Links Between Telepresence Conferences.

Basic Cascading using IP Cascaded Link

In this topology, both MCUs can be registered with the same gatekeeper or the IP addresses of both MCUs can be used for the cascading link. Content can be sent across the Cascading Link.

Basic Cascading Topology - IP Cascading Link



For example, MCU B is registered with the gatekeeper using 76 as the MCU prefix.

The connection between the two conferences is created when a dial out IP participant is defined (added) to conference A whose dial out number is the dial-in number of the conference or Entry Queue running on MCU B.

Dialing Directly to a Conference

Dial out IP participant in conference A dials out to the conference running on MCU B entering the number in the format:

[MCU B Prefix/IP address] [conference B ID].

For example, if MCU B prefix is 76 and the conference ID is 12345, the dial number is **7612345**.

Dialing to an Entry Queue

When dialing to an Entry Queue, the dial out participant dials the MCU B prefix or IP address of MCU B and the Entry Queue ID in the format:

```
[MCU B Prefix/IP address] [EQ B ID]
```

For example, if MCU B prefix is 76 and the Entry Queue ID is 22558, the dial number is 7622558.

When the participant from conference A connects to the Entry Queue, the system plays to all the participants in Conference A the IVR message requesting the participant to enter the destination conference ID.

At this point, the Conference A organizer or any other participant in the conference can enter the required information for the IVR session using DTMF codes. For example, the meeting organizer enters the destination conference ID - **12345**.

Any DTMF input from conference A is forwarded to the Entry Queue on MCU B to complete the IVR session and enable the move of the participant to the destination conference B.

Once the DTMF codes are entered and forwarded to the Entry Queue on MCU B, the IVR session is completed, the participant moved to the destination conference and the connection between the two conferences is established.

Automatic Identification of the Cascading Link

In both dialing methods, the system automatically identifies that the dial in participant is an MCU and creates a Cascading Link and displays the link icon for the participant (). The master-slave relationship is randomly defined by the MCUs during the negotiation process of the connection phase.

Basic Cascading using ISDN Cascaded Link

ISDN connection can be used to link between two MCUs or MCU and gateway and create a cascading conference. Content can be sent across the ISDN Cascading Link.



ISDN Cascaded Links are not supported when the Collaboration Server is in Ultra Secure Mode. For more information see Ultra Secure Mode.

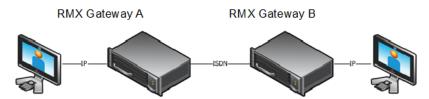
ISDN is not supported with Collaboration Server 1800.

Network Topologies Enabling Content Sharing Over ISDN Cascaded Links

ISDN Cascaded links that support content sharing can be created between two gateways, gateway-to-MCU or between two MCUs in the following network topologies:

Gateway to Gateway

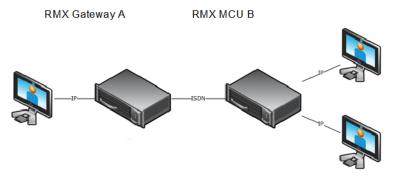
Gateway to Gateway Topology



In this topology, an IP participant calls another IP participant over an ISDN link between two gateways.

Gateway to MCU

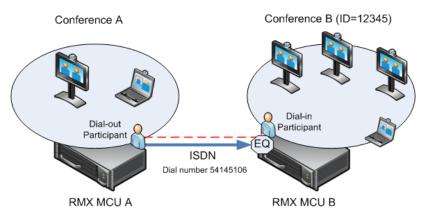
Gateway to MCU/ MCU to Gateway Topology



In this topology, an IP participant calls a conference running on an MCU via a gateway and over an ISDN link.

MCU to MCU

Cascading Between Two MCUs Using an ISDN Link



In this topology, an ISDN participant from conference running on MCU A calls a conference running on MCU B over an ISDN link.

Guidelines

- Content is restricted. When another endpoint wants to send content, the first endpoint must stop sending content before the second endpoint can initiate or send content.
- Endpoints that do not support H.239 can receive the Content using the Send Content to Legacy Endpoints option.
- When a participant joins a conference with active Content, content cannot be viewed by the new participant. Restart the Content.
- Cascaded MCUs/Gateways must be registered with the same Gatekeeper or neighboring Gatekeepers. MCUs and endpoints must also be registered with Gatekeepers.
- Gateway/MCU calls require definition of IVR Services. For more information see Defining the IVR Service for Gateway Calls.



From version 7.1, the content sharing protocol is H.263 when sent over ISDN Cascading link.

Gateway to Gateway Calls via ISDN Cascading Link

When H.323 participants connects to another IP participants via a Gateway to Gateway call over an ISDN link, the dialing string includes the following components:

[GW A prefix in GK] - The prefix with which the Collaboration Server (gateway) is registered to the gatekeeper.

[GW Profile ID] - The ID of the Gateway Profile defined on Gateway A to be used for routing the call to the Gateway B.

[GW Profile ISDN/PSTN number] - The dial-in number assigned to the Gateway Profile defined on Gateway B, including the required country and area codes.

Information required that is not part of the dialing string:

[Destination number] - The destination number as alias, IPv4 address or ISDN/PSTN number of participant B.

The dialing string format:

H.323 Participants connecting to another IP participant via a Gateway to Gateway call over an ISDN link enter a dial string using the format:

<GW A Prefix in GK><Gateway Profile_ID on GW A>*<Destination ISDN Dial-in number
assigned to the Gateway Session Profile GW B>*<Destination Number, participant>
For example:

GW A prefix in Gatekeeper - (not used with SIP)	22
Gateway Profile ID in GW A	9999
ISDN Dial-in Number assigned to the Gateway Session Profile GW B	4444103
IP Participant Alias	3456

H.323 participant dials: 229999*4444103, and when prompted for the Destination number enters 3456 followed by the pound key (#) using DTMF codes

SIP Participants connecting to another IP participant via a Gateway to Gateway call over an ISDN link enter a dial string using the format:

<Gateway Profile_ID on GW A>@<Central Signaling IP GW A>*<Destination ISDN
Dial-in number assigned to the Gateway Session Profile GW B>*<Destination
Number, participant>

For example:

If Central Signaling IP address of Gateway A is 172.22.177.89, SIP participant dials: 99990 172.22.177.89* 4444103 and when prompted for the Destination number enters 3456 followed by the pound key (#) using DTMF codes.

Gateway to MCU Calls via ISDN Cascading Link

When H.323 participants connects to a conference/Meeting Room via a Gateway to MCU call over an ISDN link, the dialing string includes the following components:

The dialing string includes the following components:

[GW A prefix in GK] - The prefix with which Gateway A is registered to the gatekeeper.

[GW Profile ID on GW A] - The ID of the Gateway Profile on GW A to be used for routing the call to the Meeting Room/conference running on MCU B.

[Conference/Meeting Room/Entry Queue ISDN/PSTN number] - The dial-in number assigned to the Entry Queue/Meeting Room/Conference defined on MCU B, including the required country and area codes.

Information required that is not part of the dialing string:

[Destination Conference ID] - Only if using the Entry Queue on MCU B for routing calls or creating new ad hoc conferences. The ID of the destination conference on MCU B.

The dialing string format:

<GW A Prefix in GK><Gateway Profile_ID on GW A>*<ISDN Number assigned to the Meeting Room/Conference/Entry Queue>

For Example:

GW A prefix in Gatekeeper - (not used with SIP)	22
Gateway Profile ID in GW A	9999
ISDN Dial-in Number assigned to the Entry Queue/MR/conference	4444100
H.323 participant dials	229999*4444100

SIP participant dials (if Central Signaling IP address of Gateway A is 172.22.177.89) 99990 172.22.177.89 IP* 4444100

If dialing an Entry Queue, when prompted for the Destination number enters 3456 followed by the pound key (#) using DTMF codes to create a new conference or join an ongoing conference with that ID.

MCU to MCU Calls via ISDN Cascading Link

A dial out ISDN participant is defined (added) to conference A running on MCU A. The participant's dial out number is the dial-in number of the Entry Queue or conference running on MCU B (for example 54145106).

MCU A dials out to an Entry Queue or conference B running on MCU B using the Entry Queue number (for example 54145106) or the conference number.

When the participant, who is a dial-in participant in conference B, connects to the Entry Queue, the system plays to all the participants in Conference A the IVR message requesting the participant to enter the destination conference ID (or if connecting to a conference directly, the participant is requested to enter the conference password).

At this point the Conference A organizer or any other participant in the conference can enter the required information for the IVR session using DTMF codes. For example, the meeting organizer enters the destination conference ID - 12345.

Any DTMF input from conference A is forwarded to the Entry Queue on MCU B to complete the IVR session and enable the move of the participant to the destination conference B.

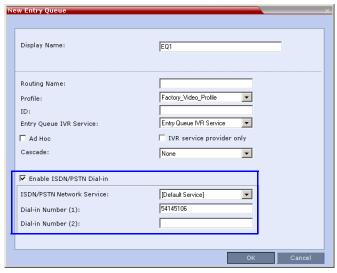
Once the DTMF codes are entered and the IVR session is completed, the participant is connected to the conference and the connection between the conferences is established. The system automatically identifies the calling participant as an MCU and the connection is identified as a cascading link and the cascading link icon is displayed for the participant (§).

Collaboration Server Configuration Enabling ISDN Cascading Links

To enable Gateway-to-Gateway, Gateway-to-MCU and MCU-to-MCU calls over ISDN Cascading links, the following configurations are required:

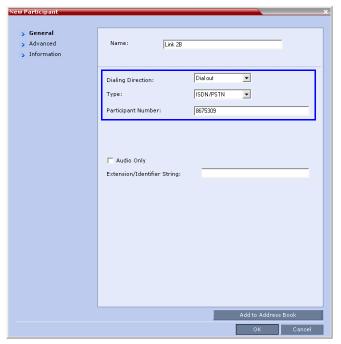
Modifying the IP Network Service to include the MCU Prefix in the Gatekeeper (in the Gatekeepers dialog box). For more details, see Modifying the Default IP Network Service.

- ISDN Network Service is configured in both MCUs. For more details, Modifying an ISDN/PSTN Network Service.
- Configuring a Gateway Profile and assigning dial-in ISDN/PSTN numbers. For details, see Defining the Gateway Profile.
- Configure the Entry Queue or conference (for direct dial-in) as enabled for ISDN connection and a dial-in number is assigned (for example 54145106).



 Defining the dial-in ISDN participant in MCU B and Dial-out ISDN participant in MCU A (for MCU-to-MCU cascading conferences).

A dial out ISDN participant is defined (added) to conference A. The participant's dial out number is the dial-in number of the Entry Queue or conference running on MCU B (for example 54145106).

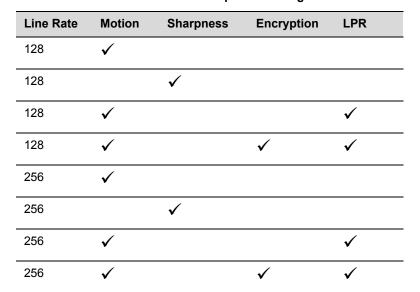


MCU A dials out to an Entry Queue or conference B running on MCU B using the Entry Queue number (for example 54145106) or the conference number.

Conference Profile Definition

The following table lists the recommended Meeting Room/Conference Profile parameters setting when routing ISDN cascaded calls.

Recommended Conference Profile Options Setting



Recommended Conference Profile Options Setting

Line Rate	Motion	Sharpness	Encryption	LPR
384	✓			
384		✓		
384	✓			✓
384	✓		✓	✓
512	✓			
512		✓		
512	✓			✓
512	✓		✓	✓
768	✓			
768		✓		
768	✓			✓
768	✓		✓	✓



Since the remote participant settings are unknown, it is recommended that the gateway or endpoint be configured to support a higher line rate (for example, 768 Kbps) to allow flexibility during endpoint capability negotiations.

MCU Interoperability Table

The following table lists the different MCU and Gateway configurations that are supported or implemented when routing Cascaded ISDN calls.

MCU Interoperability Table

		Scenario	Version(s)
Collaboration Server Gateway	Collaboration Server MCU	User calls via a Gateway to a Remote Conference (user to conference)	Collaboration Server v. 7.1 or later
Collaboration Server Gateway	Collaboration Server Gateway	User calls via a Gateway to a Remote User behind Gateway (user to user)	Collaboration Server v. 7.1 or later
Collaboration Server MCU	Collaboration Server MCU	A dial out participants calls to a remote conference (conference to conference)	Collaboration Server v. 7.1 or later

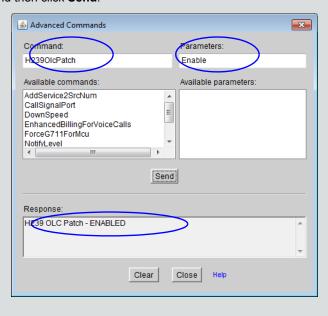
MCU Interoperability Table (Continued)

		Scenario	Version(s)
Collaboration Server MCU	Collaboration Server Gateway	A dial out participants calls to a remote User behind a Gateway (Conference to User)	Collaboration Server v. 7.1 or later
Endpoint	Collaboration Server Gateway	User calls directly to a remote user behind a Gateway (User to User)	Collaboration Server v. 7.1
Collaboration Server MCU	Codian Gateway	Dial out participants use a fixed rule behind the Codian Gateway.	Collaboration Server v. 7.1 Latest Codian version
Collaboration Server Gateway	Codian Gateway	Dial out participants use a fixed rule behind the Codian Gateway.	Collaboration Server v. 7.1 Latest Codian version
Codian Gateway	Collaboration Server MCU	User calls via a Codian Gateway to a Remote Conference (user to conference)	Collaboration Server v. 7.1 Latest Codian version
Codian Gateway	Collaboration Server Gateway	User calls via a Codian Gateway to a Remote User behind Collaboration Server Gateway (user to user)	Collaboration Server v. 7.1 Latest Codian version
Collaboration Server MCU	Radvision Gateway	User calls via a Radvision Gateway to a Remote User behind Collaboration Server Gateway (user to user)	Collaboration Server v. 7.1 Latest Radvision version
Collaboration Server Gateway	Radvision Gateway	User calls via a Radvision Gateway to a Remote User behind Collaboration Server Gateway (user to user)	Collaboration Server v. 7.1 Latest Radvision version
Radvision Gateway	Collaboration Server MCU	User calls via a Radvision Gateway to a Remote Conference (user to conference)	Collaboration Server v. 7.1 Latest Radvision version
Radvision Gateway	Collaboration Server Gateway	User calls via a Radvision Gateway to a Remote User behind Collaboration Server Gateway (user to user)	Collaboration Server v. 7.1 Latest Radvision version
Endpoint	Collaboration Server Gateway	User calls directly to a DMA controlled environment	Collaboration Server v. 7.1
Collaboration Server MCU	Collaboration Server Gateway	A dial out participants calls to a remote conference on a DMA controlled environment	Collaboration Server v. 7.1



- On the Codian gateway Content is not supported with line rates of 128Kbps and below.
- When using the following topology:
 H.323 endpoint > Codian Gateway > ISDN Link Collaboration Server > H.323 endpoint, the Codian Gateway is unable to send DTMF and the call is disconnected (VNGFE- 3587).
- Sending Content from a participant over Radvision Gateway to a conference/participant, the GWP20 patch must be installed in the RadVision gateway:

On the Radvision gateway, open the GWP20 User Interface. Select **Settings > Advanced Commands**. In the **Command** box enter **H239OlcPatch**. In the **Parameters** box enter **Enable** and then click **Send**.



Suppression of DTMF Forwarding

Forwarding of the DTMF codes from one conference to another over an ISDN cascading link is not automatically suppressed as with IP cascading link and it can be limited to basic operations while suppressing all other operations by a system flag **DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS**.

System Flag Settings

The **DTMF_FORWARD_ANY_DIGIT_TIMER_SECONDS** flag determines the time period (in seconds) that MCU A will forward DTMF inputs from conference A participants to MCU B.

Once the timer expires, most of the DTMF codes (excluding five operations as for IP links) entered in conference A will not be forwarded to conference B. This is done to prevent an operation requested by a participant individually (for example, mute my line) to be applied to all the participants in conference B.

Flag range (in seconds): 0 - 360000

This flag is defined on MCU A (the calling MCU).

If a flag is not listed in the *System Flags* list it must be added to the *system.cfg* file before it can be modified. For more details on defining system flags, see Modifying System Flags.

Star Cascading Topology

In the Star topology (as well as in the Basic topology), the MCUs are usually installed at different locations (states/countries) and participants connect to their local MCU to facilitate the connection and save long distance call costs. Star Topology Cascading requires that all cascaded MCUs reside on the same network.



Although participants in Star Cascading conferences can connect to their local conference using IP (H.323, SIP) and ISDN, the Cascading Links between conferences must connect via H.323.

Content sharing is available to all conferences over the H.323 Cascading Link.

In this topology, the MCUs are networked together using two modes:

- Master-Slave Cascading
- · Cascading via Entry Queue

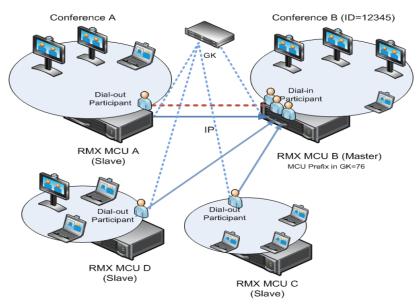
Master-Slave Cascading

It is similar to MIH (Multi Hierarchy) cascading, with only two levels: one Master MCU on level 1 and several Slave MCUs on level 2.

The cascading hierarchy topology can extend to four levels (MIH Cascade - a Sample 3-Level Cascading Configuration) and should be deployed according to the following guidelines:

- If an Collaboration Server is deployed on level 1:
 - Collaboration Server systems can be used on level 2
 - ➤ MGC with version 9.0.4 can be used on level 2 if Collaboration Server version 7.0.2 and higher is deployed in level 1
- If an MGC is deployed on level 1:
 - MGC or Collaboration Server can be used on level 2.

Master-Slave Star Cascading Topology



- When creating a cascading link between two Collaboration Servers:
 - > The Collaboration Servers operate in CP (Continuous Presence) mode.
- When creating a cascading link between MGCs and Collaboration Servers:
 - > The MGCs can only operate in VSW mode (not supported with Collaboration Server 1800).

The following table summarizes Video Session Modes line rate options that need to be selected for each conference in the cascading hierarchy according to the cascading topology:

MIH Cascading - Video Session Mode and Line Rate

Topology	MCU Type	Video Session Mode	Line Rate	Endpoint
Level 1	Collaboration Server	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s	HDX
Level 2	Collaboration Server	-		
Level 1	Collaboration Server	CP - CIF	768Kb/s, 2Mb/s	VSX
Level 2	Collaboration Server	-		
Level 1	MGC	CP - CIF 263	768Kb/s, 2Mb/s	HDX, VSX
Level 2	Collaboration Server	CP - CIF 264	-	
Level 1	MGC	VSW - HD	1.5Mb/s	HDX
Level 2	Collaboration Server	VSW - HD	_	

To establish the links between two Collaboration Servers requires the following procedures be performed:

 Establish the Master-Slave relationships between the cascaded conferences by defining the dialing direction.

- Create the Master and Slave conferences, defining the appropriate line rate.
- Create a cascade-enabled Dial-out Participant link in the Master conference
- Create a cascade-enabled Dial-in Participant link in the Slave conference.

Creating a Cascade Enabled Dial-out/Dial-in Participant Link

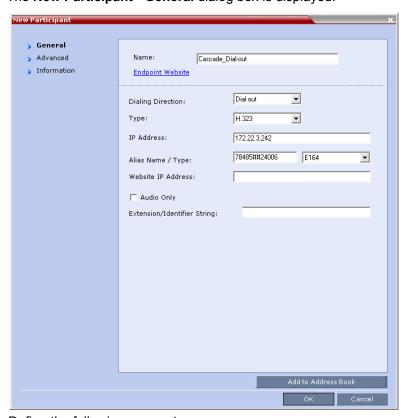
The connection between two cascaded conferences is established by a cascade enabled dial-out and dial-in participants, acting as a cascades link.

The dialing direction determines whether the dial-out participant is defined in the conference running on the Master MCU or the Slave MCU. For example, if the dialing direction is from the Master conference on level 1 to the Slave conference on level 2, the dial-out participant is defined in the Master conference on level 1 and a dial-in participant is defined in the Slave conference running on the MCU on level 2.

If the cascade-enabled dial-out participant always connects to the same destination conference on the other (second) MCU, the participant properties can be saved in the Address Book of the MCU for future repeated use of the cascaded link.

To define the dial-out cascade participant link:

- 1 In the **Conferences** pane, select the conference.
- 2 In the Participants pane, click New Participant ().
 The New Participant General dialog box is displayed.

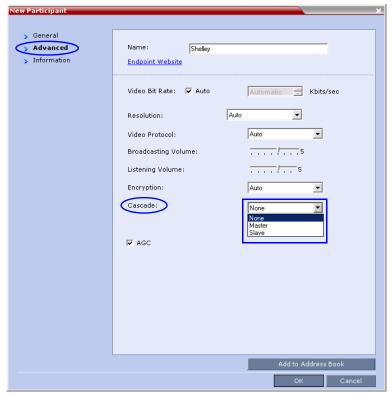


3 Define the following parameters:

New Participant - Dial-out Cascade Link

Field	Description
Name	Enter the participant's name. This field may not be left blank. Duplicate participant names, comma, and semi-colon characters may not be used in this field.
Dialing Direction	Select Dial-out.
Туре	Select H.323.
IP Address	Enter the IP address of the Signaling Host of the MCU running the other (second) conference, where the cascade enabled Entry Queue is defined.
Alias Name	If you are using the target MCU IP address, enter the Conference ID of the target conference. For example: 24006
	If a gatekeeper is used, instead of the IP address, you can enter the prefix of the target MCU as registered with the gatekeeper, as part of the dialing string and the conference ID in the format:
	<target mcu="" prefix=""><conference_id></conference_id></target>
	For example: 925 24006
	If the conference has a password and you want to include the password in the dial string, append the password to in the dial string after the Conference ID.
	For example: 92524006##1234
	If the conference has a password and you do not want to include the password in the dial string, set the ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD flag to YES .
	For more information see Modifying System Flags.
Alias Type	Select E.164 (digits 0-9, *, #).

4 Click the Advanced tab.

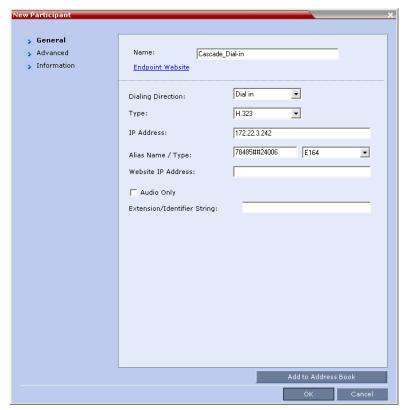


- 5 In the Cascade field, select:
 - > Slave, if the participant is defined in a conference running on a Slave MCU.
 - > Master, if the participant is defined in a conference running on the Master MCU.
- 6 Click OK.

To define a Dial-in Participant as the cascade link:

This participant is added to the ongoing conference on the Slave MCU.

1 In the Participants list, click the New Participant button(). The New Participant - General dialog box opens.



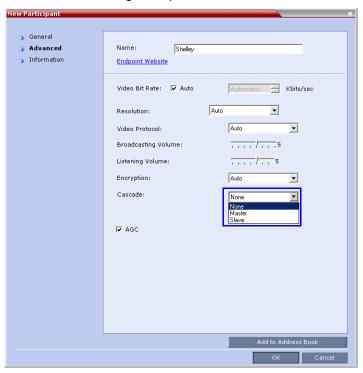
2 Define the following parameters:

New Participant - Dial-in Cascade Link

Field	Description	
Display Name	Enter the participant's name.	
	This field may not be left blank. Duplicate participant names, comma, and semi-colon characters may not be used in this field.	
Dialing Direction	Select Dial-in.	
Туре	Select H.323.	
IP Address	If a gatekeeper is used: This field is left empty.	
	If a gatekeeper is not used: Enter the IP address of the Signaling Host of the MCU running the other conference.	
Alias Name	If a gatekeeper is used: Enter the name of the other (second) conference.	
	If a gatekeeper is not used: Enter the ID of the MCU running the other (second) conference.	
Alias Type	If a gatekeeper is used: H.323 ID	
	If a gatekeeper is not used: Select E.164 (digits 0-9, *, #).	

3 Click the Advanced tab.

The Advanced dialog box opens.

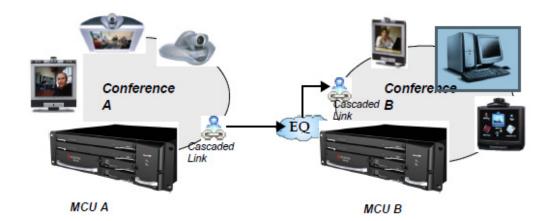


- 4 In the Cascaded Link field, select:
 - > Slave, if the participant is defined in a conference running on a Slave MCU.
 - > Master, if the participant is defined in a conference running on the Master MCU.
- 5 Click the **OK** button.

Cascading via Entry Queue

The link between the two conferences is created when a participant that is defined as a dial-out cascaded link in one conference (Conference A) connects to the second conference (Conference B) via a special cascaded Entry Queue (EQ). When MCU A dials out to the cascaded link to connect it to conference A, it actually dials out to the cascaded Entry Queue defined on MCU B.

Cascaded Conferences - Star Topology



Though the process of cascading conferences mentioned in this section refers to conferences running on two different Collaboration Server units, it is possible to cascade conferences running between Collaboration Server units and other MCUs.

The following features are not supported by the cascaded link and therefore are not supported in the combined conference:

- **DTMF** codes are enabled in cascaded conference, but only in their local conference. The operations executed via DTMF codes are not forwarded between linked conferences.
- FECC (Far End Camera Control will only apply to conferences running in their local MCU).

Enabling Cascading

Cascading two conferences requires that the following procedures are implemented:

- Creating the cascade-enabled Entry Queue
 - A cascade-enabled Entry Queue must be created in the MCU hosting the destination conference (Conference B). The cascade-enabled Entry Queue is used to establish the dial-in link between the destination conference and the linked conference and bypassing standard Entry Queue, IVR prompt and video slide display.
- Creating a cascade-enabled Dial-out link
 - The creation of a cascade-enabled dial-out link (participant) in the linked conference (Conference A). This dial-out participant functions as the link between the two conferences.
- (Optional) Enabling the cascaded linked participant to connect to the linked conference (Conference
 A) without entering the conference password. This can be done by modifying the default settings of
 the relevant system flag.

Creating the Cascade-enabled Entry Queue



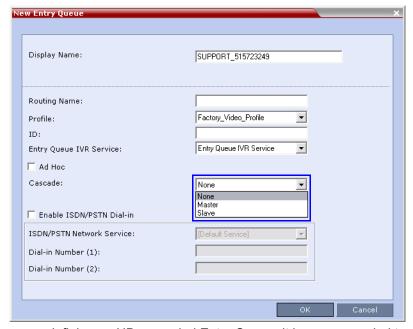
The cascade-enabled Entry Queue should be used only to connect cascaded links and should not be used to connect standard participants to conferences.

The cascade-enabled Entry Queue maintains the correct behavior of the cascaded link when it dials into it.

When cascading High Definition (HD) conferences, the cascade-enabled Entry Queue must have the same settings as both cascaded conferences and the participants in both conferences must use the same line rate and HD capabilities as set for the conferences and Entry Queue.

To Define a Cascade-Enabled Entry Queue:

- 1 In the Collaboration Server Management pane, click the Entry Queues button.
 - The **Entry Queues** list pane is displayed.
- 2 Click the **New Entry Queue** description.
 - The **New Entry Queue** dialog box is displayed.
- **3** Define the standard Entry Queue parameters (as described in Chapter 3).
- 4 In the Cascade field, select Master or Slave depending on the Master/Slave relationship.
 - > Set this field to **Master** if the Entry Queue is defined on the MCU that is at the center of the topology and other conferences dial into it (acting as the Master).
 - > Set this field to **Slave** if the Entry Queue is defined on the MCU acting as a Slave, that is, to which the link from the Master MCU (MCU at the center of the topology) is dialing.



If you are defining an HD cascaded Entry Queue, it is recommended to select the same Profile that is selected for both conferences.

5 Click OK.

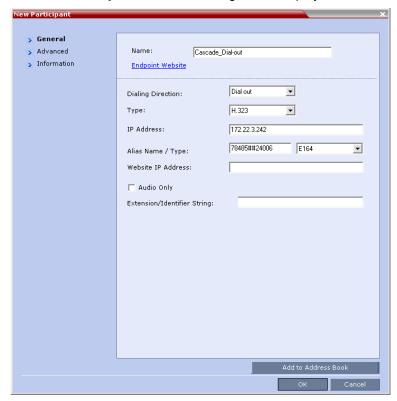
The new Entry Queue enabling cascading is created.

Creating the Dial-out Cascaded Link

The dial-out link (participant) is created or added in the linked conference (Conference A). The dial-out string defined for the participant is the dialing string required to connect to the destination conference (Conference B) Entry Queue defined on the MCU hosting the destination cascaded conference. The dial-out participant can be defined in the Address Book and added to the conference whenever using the same cascade-enabled Entry Queue and a destination conference (with the same ID and Password).

To define the Dial-out Cascaded Link:

- 1 Display the list of participants in the linked conference (Conference A).
- 2 In the Participant List pane, click the New Participant button.
 The New Participant General dialog box is displayed.



- 3 In the Name field, enter a participant name.
- 4 In the Dialing Direction field, select Dial-out.
- 5 In the Type list field, verify that H.323 is selected.
- **6** There are two methods to define the dialing string:
 - a Using the MCU's IP Address and the Alias string see Method A.

b Using only the Alias string (requires a gatekeeper) - see Method B.

Method A

In this method no gatekeeper is used.

In the **IP Address** field, enter the IP address of the **Signaling Host** of the MCU hosting the destination conference (in the example, MCU B).

In the **Alias Name/Type** field, enter the ID of the cascade-enabled Entry Queue (EQ), the Conference ID and Password of the destination conference (MCU B) as follows:

<EQ ID>#<Destination Conference ID>#<Password> (Password is optional).

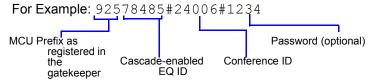


Method B

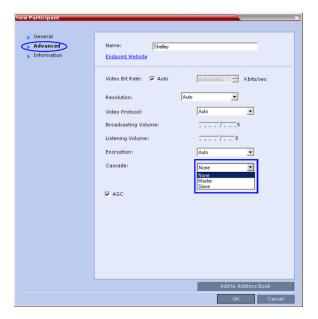
In this method a gatekeeper is used:

In the **Alias Name** field, enter the Prefix of MCU B, EQ ID, Destination Conference ID, and Password, as follows:

<MCU Prefix EQ ID>#<Conference ID>#<Password> (Password is optional)



- 7 Click the Advanced tab.
- 8 In the Cascade field, select:
 - Slave, if the participant is defined in a conference running on a Slave MCU and will connect to the Master MCU (in the center of the topology).
 - ➤ **Master**, if the participant is defined in a conference running on the Master MCU (in the center of the topology) dialing from the Master MCU to the Slave MCU.



9 Click OK.

The cascade-enabled dial-out link is created and the system automatically dials out to connect the participant to the linked conference, as well as the destination conference.

Enabling Cascaded Conferences without Password

If a password is assigned to the linked conference, cascaded links will be prompted for a password when connecting to it (Conference A). Administrators have the option of altering the MCU settings to enable cascaded links to connect without a password.

To enable cascaded links to connect without a password:

- 1 In the Collaboration Server web client connected to MCU A (where the linked conference is running), click Setup>System Configuration.
 - The **System Flags** dialog box opens.
- 2 Set the ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD flag to YES.
- 3 Click OK.

For more information, see Modifying System Flags.

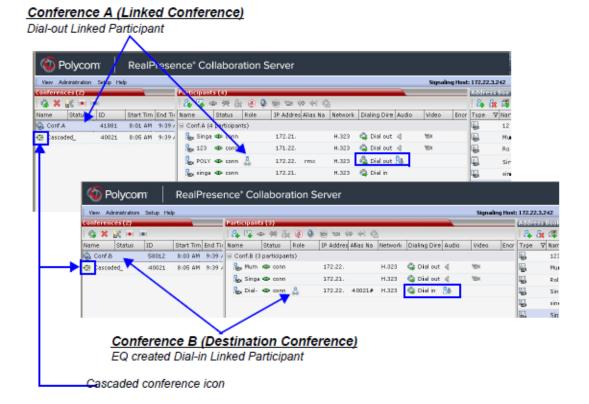
Reset the MCU for flag changes to take effect.

Monitoring Star Cascaded Conferences

To monitor both conferences at the same time, two instances of the Collaboration Server Web Clients must be opened (one for each MCU) by entering the IP Address of each MCU. If both conferences are running on the same MCU, only one Collaboration Server Web Client window is required.

When conferences are cascaded, the **Participant List** pane of each of the two conferences will display a linked icon (ﷺ); a dial-in linked icon in the destination conference (Conference B) and a dial-out linked icon in the linked conference (Conference A).

The **Conferences List** panes in each of the two conferences will display a cascaded conference icon (indicating that a conference running on the MCU is presently cascading with another conference running on the same or another MCU. The cascaded conference icon will be displayed for a short period of time and then disappear.

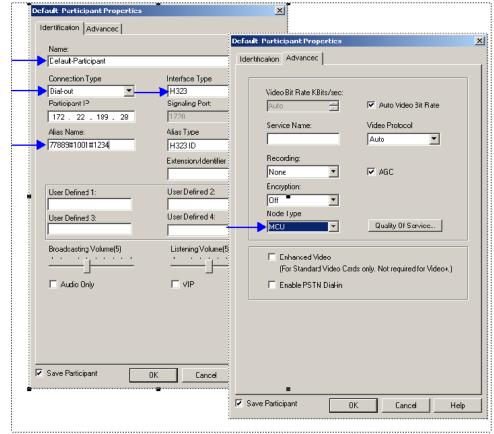


Creating the Dial-out Link from a Conference Running on the MGC to the Conference Running on the Collaboration Server

In the same way that the dial-out cascaded link is created in the Collaboration Server, you can create a dial-out participant in the MGC.

In the MGC Manager application, define a new participant as follows:

- 1 In the Participant Properties dialog box, enter a Participant Name, select Dial-out and H.323.
- 2 Define the **dialing string** as described in step 6 in the procedure for defining the dial-out cascaded link.



3 In the Advanced tab, in the Node Type field, select MCU.

4 Click OK.

Cascading Conferences - H.239-enabled MIH Topology

H.239 Multi-Hierarchy (MIH) cascading is available to Collaboration Server users enabling them to run very large conferences on different MCUs in multiple levels of Master-Slave relationships using an H.323 connection.

Multi-Hierarchy (MIH) Cascading is implemented where the cascaded MCUs reside on different networks, whereas Star Topology Cascading requires that all cascaded MCUs reside on the same network.

MIH Cascading allows:

- Opening and using a content channel (H.239) during conferences.
- Full management of extremely large, distributed conferences.
- Connecting conferences on different MCUs at different sites.
- Utilizing the connection abilities of different MCUs, for example, different communication protocols, such as, serial connections, ISDN, etc.
- Significant call cost savings to be realized by having participants call local MCUs which in turn call remote MCUs, long distance.

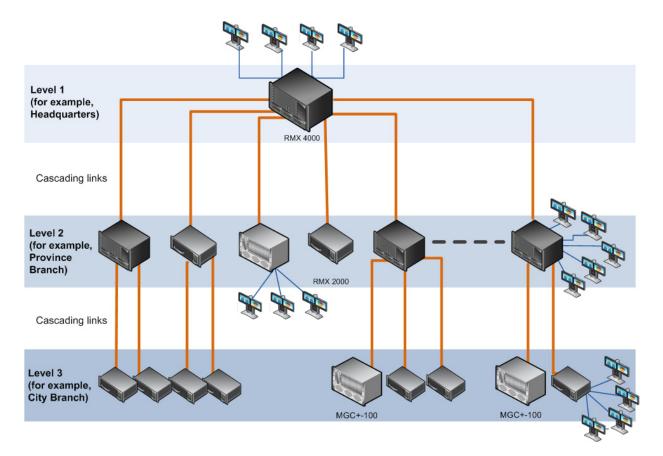


Although participants in MIH Cascading conferences can connect using IP (H.323, SIP) and ISDN, the MIH Cascading Links must connect via H.323.

MIH Cascading Levels

The cascading hierarchy topology can extend to up to four levels (as shown below), where the most common configuration includes up to three levels.

MIH Cascade - a Sample 3-Level Cascading Configuration



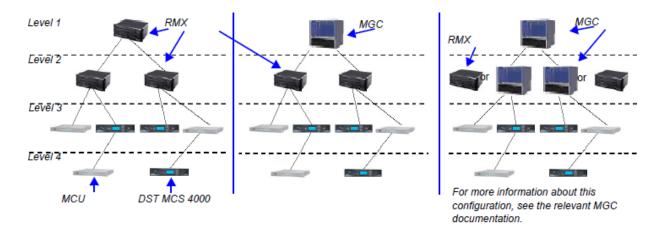
Cascading Topologies

The cascading hierarchy topology should be deployed according to the following guidelines:

- If an RMX is deployed on level 1 (recommended deployment):
 - Any RMX can be used on level 2, 3 and 4 (recommended deployment),
 - ➤ MGC version 9.0.4 can be used on level 2 and level 3,
 - > DST MCS 4000 and other MCUs can be deployed on levels 3 and 4.
- If an MGC is deployed on level 1:
 - > MGC or RMX can be used on level 2.

- > DST MCS 4000 and other MCUs can be deployed on levels 3 and 4.
- DST MCS 4000 MCUs connect as endpoints to the RMXs or MGCs on higher levels.

MIH Cascade Levels

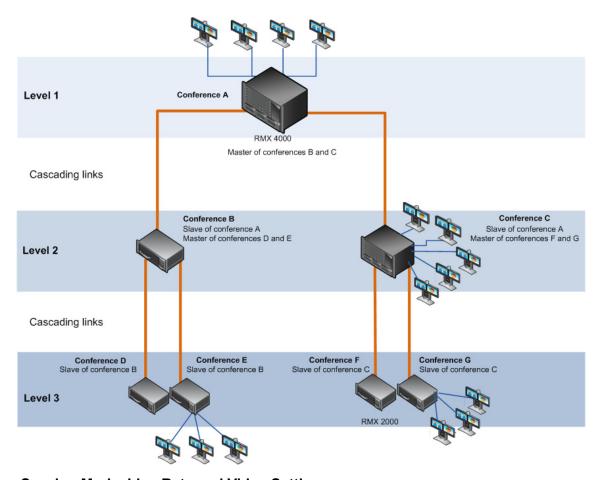


MIH Cascading Guidelines in CP Licensing

Master - Slave Conferences

- It is recommended to have RMX systems at all levels to leverage the high quality video and content offered by the RMX.
- In MIH Cascading conferences, although there are multiple levels of Master and Slave relationships between conferences, the conference that runs on the MCU on level 1 of the hierarchy must be the Master for the entire cascading session. When an MGC is part of the cascading topology, it can be configured at any level if MGC Version 9.0.4 is installed, otherwise, it must be set as Level 1 MCU.
- Conferences running on MCUs on levels 2 and 3 and can be both Masters and Slaves to conferences running on MCUs on levels above and below them.
- All conferences running on MCUs on the lowest level in the configuration (for example, level 3 in a 3-level hierarchy configuration) are Slave conferences.
- When the DST MCS 4000 is on level 3 and acting as slave to level 2, the RMX on level 2 must dial
 out to it in order for the DST MCS 4000 to be identified as slave. The link between the two MCU (dial
 out participant) is defined as a standard participant and not as a cascading link.

MIH Cascading - Master-Slave Relationship



Video Session Mode, Line Rate and Video Settings

The types of MCUs, their position in the cascade topology and the endpoint capabilities (HD/CIF and H.263/H.264) determine the Video Session Type of the MIH Cascading conference.

- When creating a cascading link between two RMXs:
 - ➤ The RMXs operate in CP (Continuous Presence) mode.
 - ➤ DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences.
- When creating a cascading link between MGCs and RMXs:
 - > If there are no MGCs on level 2, the MGCs can operate in either in CP or VSW (Video Switching) mode.
 - ➤ If there are MGCs on level 2, the MGCs can only operate in VSW mode.
 - ➤ MGC does not support H.264 High Profile, therefore when MGC is part of the Cascading topology, do not select High Profile on the RMX system.
 - DTMF codes should be defined with the same numeric codes in the IVR services assigned to the cascading conferences.

- When creating a cascading link between two MGCs the MGCs must be configured to operate in VSW mode.
 - For more details about the MGC to MGC connection, see the MGC Manager User's Guide, Volume II, Chapter 1, Ad Hoc Auto Cascading and Cascading Links.
- To enable the connection of the links between cascaded conferences, they must run at the same line rate.
- To enable Content sharing between the RMX and the MGC, the rate allocated to the content must be
 identical in both conferences. Make sure that the line rate set for both conferences, and the Content
 Settings (Graphics, Hi-res Graphics or Live video) are selected correctly to ensure the compatible
 rate allocation. For more details on the RMX rate allocation to the Content channel, see SIP BFCP
 Content Capabilities.

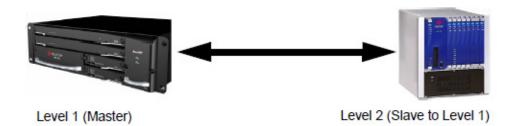
The following table summarizes Video Session Modes line rate options that need to be selected for each conference in the cascading hierarchy according to the cascading topology:

MIH Cascading - Video Session Mode and Line Rate

MCU Type	Video Session Type	Line Rate
RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
RMX		
RMX	CP - CIF	768Kb/s, 2Mb/s
RMX		
RMX	СР	768Kb/s, 2Mb/s
MGC	CP or VSW	
MGC	CP - CIF 263	768 kb/s, 2Mb/s
RMX	CP - CIF 264	
MGC	VSW - HD	1.5Mb/s
RMX	VSW HD	
RMX	CP - HD	1.5Mb/s, 1Mb/s, 2Mb/s
RMX		
MGC	VSW*	384 kbps, 768 kbps
MGC		
RMX	CP/VSW -HD	1.5Mb/s, 1Mb/s, 2Mb/s
MCS 4000		
RMX	CP - CIF	768kb/s, 2Mb/s
MCS 4000		
	RMX RMX RMX RMX RMX RMX RMX MGC MGC RMX MGC RMX MGC RMX	RMX CP - HD RMX CP - CIF RMX CP RMX CP MGC CP or VSW MGC CP - CIF 263 RMX CP - CIF 264 MGC VSW - HD RMX VSW HD RMX CP - HD RMX VSW* MGC VSW* MGC CP/VSW - HD MCS 4000 CP - CIF

^{*} When MGC is on Level 3, Content cannot be shared between Level 2 and Level 3.

MGC to Collaboration Server Cascading



If MGC is running version 9.0.4, and Collaboration Server is running version 7.0.2 and higher, the Collaboration Server can be set as Master on level 1 and MGC as Slave on level 2.

MGC running versions other than 9.0.4 is always on level 1 and must be set as the Master MCU.

If the cascading topology includes additional MGCs as well as Collaboration Servers it is recommended to define Video Switching conferences for all the cascading conferences running on the MGC in the topology.

Two methods can be used to create the Cascading links between conferences running on the Collaboration Server and MGC:

- Method I Establish the links by defining a dial-in and a dial-out participant in the Slave and Master conference (where the Master conference is created on the MCU on Level 1 and the Slave conference is created on the MCU on Level 2).
- Method II Using a Cascading Entry Queue on either the MGC or the Collaboration Server depending on the dialing direction and the MCU Level. This is recommended when the Collaboration Server is on Level 1.

Method I

Depending on the dialing direction, the following procedures must be performed:

Set up Procedures according to the Dialing Direction

Dialing Direction	Collaboration Server - Level 1	MGC - Level 2
MGC to Collaboration Server	Set the appropriate flags (done once only).	Set the appropriate flags (done once only).
	Define the conference setting and its line rate to be the same as the one set on the Collaboration Server.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-in participant (Cascaded Link) with the calling number from the MGC. The alias that will be used to identify the dial-in participant can be the name of the calling slave conference. Set the Cascading option as Master.	Define the dial-out participant (Cascaded Link) to the conference running on the Collaboration Server. Set the dial-out alias to be the prefix of the MCU and the name of the master conference running on the Collaboration Server.

Set up Procedures according to the Dialing Direction

Dialing Direction	Collaboration Server - Level 1	MGC - Level 2
Collaboration	Set the appropriate flags (done once only)	Set the appropriate flags (done once only)
Server to MGC	Define the conference setting and its line rate to be the same as the one set on the Collaboration Server.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-out participant (Cascaded Link). Set the dial-out alias to be the prefix of the MGC and the name of the slave conference running on the MGC. Set the Cascading option as Master.	Define the dial-in participant (Cascaded Link) to the conference running on the Collaboration Server. The alias that will be used to identify the dial-in participant can be the name of the calling slave conference.

For details on the participant definition on the Collaboration Server, see Creating a Cascade Enabled Dial-out/Dial-in Participant Link.

For a detailed description of the participant definition in the MGC, see the MGC Manager User's Guide, Volume II, Chapter 1, Cascading Conferences.



To enable Content sharing between the Collaboration Server and the MGC, the rate allocated to the content must be identical in both conferences. Make sure that the line rate set for both conferences, and the Content Settings (Graphics, Hi-res Graphics or Live video) are selected correctly to ensure the compatible rate allocation. For more details on the Collaboration Server rate allocation to the Content channel, see SIP BFCP Content Capabilities.

Method II

Depending on the dialing direction, the following procedures must be performed:

Set up Procedures according to the Dialing Direction

Dialing Direction	MGC Level 1	RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Level 2
MGC to Collaboration Server	Set the appropriate flags (done once only).	Set the appropriate flags (done once only).
Server		Define the cascade-enabled Entry Queue, setting it as Slave .
	Define the conference setting and its line rate to be the same as the one set on the Collaboration Server.	Define the conference setting and its line rate to be the same as the one set on the MGC.
	Define the dial-out participant (Cascaded Link) to the conference running on the Collaboration Server.	

Set up Procedures according to the Dialing Direction

Dialing Direction	MGC Level 1	RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Level 2
Collaboration	Set the appropriate flags (done once only)	Set the appropriate flags (done once only)
Server to MGC	Define the cascade-enabled Entry Queue.	
	Define the conference setting and its line rate to be the same as the one set on the Collaboration Server.	Define the conference setting and its line rate to be the same as the one set on the MGC.
		Define the dial-out participant (Cascaded Link) to the conference running on the MGC, setting the participant Cascade parameter to Slave .

Setting Flags on the Collaboration Server

When running conferences in mixed environment (Collaboration Server and MGC) there may be small differences between the line rates each MCU is sending. In the Collaboration Server, several flags must be set to ensure that these differences will not cause the cascaded link to connect as Secondary and that Content flows correctly between the cascaded conferences. This procedure is performed once per Collaboration Server.

To modify the flags:

- 1 In the Collaboration Server Web Client menu, click Setup>System Configuration.
- 2 In the **System Flags** dialog box, add the following new flags and values:
 - > MIX_LINK_ENVIRONMENT=YES

Setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the RealPresence Collaboration Server 1800 from 1920Kbps to 17897Kbps to match the actual rate of the HD Video Switching conference running on the MGC. In such case, the conference can include IP and ISDN participants.

> IP_ ENVIRONMENT_LINK=NO



If the flag MIX_LINK_ENVIRONMENT is set to YES, the IP_LINK_ENVIRONMENT flag must be set to NO.

If the flag MIX_LINK_ENVIRONMENT is set to NO, the IP_LINK_ENVIRONMENT flag must be set to YES.

> H263_ANNEX_T=YES (default)

This flag enables/disables the use of Annex T with H263. Set it to **NO** if the endpoints connecting to the conference do not support this mode. In such a case, you must also change the MGC flag **ENABLE_H239_ANNEX_T** setting to **NO**.

> FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION=YES (default).

Set this flag to **NO** If the MGC is functioning as a Gateway and participant layouts on the other network are not to be forced to 1X1.

- 3 If the MGC is dialing the Collaboration Server and the cascaded link connects to the conference via the Cascade-enabled Entry Queue without being prompted for the conference password, set the flag to YES as follows: ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD=YES
- 4 Click OK.
- **5** Reset the MCU to apply the changes.

Setting Flags in the MGC

Flag setting is required to ensure the correct MCU behavior for cascading conferences. It is performed once per MCU.

To modify the flags:

- 1 In the MGC Manager, right-click the MCU icon and then select MCU Utils > Edit "system.cfg".
- 2 In the **H264 Section**, ensure that the following flags are set to:
 - > ENABLE_HD_SD_IN_FIXED_MODE=YES

Setting this flag to YES enables H.264 Standard Definition (SD), High Definition (HD) and VSX 8000 (Version 8.0) support in Video Switching conferences.

> H264_VSW_AUTO=NO

Setting this flag to NO disables the highest common mechanism in H.264 and enables the selection of H.264 Video Protocol in fixed mode in Dual Stream Video Switching cascading conferences.

ENABLE_H239_ANNEX_T=YES

This flag should be set to the same value (YES/NO) as the settings of the Collaboration Server flag H263_ANNEX_T.



To use MIH Cascade in the MGC, the Conference Numeric ID routing mode must be used. It is determined when the **system.cfg** flag in the **GREET AND GUIDE/IVR** section is set to **QUICK_LOGIN_VIA_ENTRY_QUEUE=NO**.

- 3 Click OK.
- 4 If you changed the flags, reset the MCU.

Method II - Defining the Cascading Entry Queue in the MGC

The Entry Queue definition on the MGC is required if the dialing is done from the Collaboration Server to the MGC.

- 1 In the MGC Manager, expand the MCU tree.
- 2 Right-click the Meeting Rooms, Entry Queues and SIP Factories icon and click New Entry Queue.

X Entry Queue Settings Cascade EQ Entry Queue Service: EQ80 • Numeric ID: 1002 ▼ Cascade VTX 1000 Target Conference Settings ☐ Ad Hoc 56 (G722/G711) • Audio Ala: Profile | Y Video Format: Auto Target Conferences Frame Rate: Auto w Audio Only • Video Protocol: Auto ☐ IP Only ☐ Encryption □ Annex N □ Annex P Video Switching Line Rate: 768 kbps ☐ Restricted C Transcoding C Continuous Presence Service Name Dial-in Number (1) Dial-in Number (2) OK Cancel

3 In the New Entry Queue dialog box, set the Entry Queue parameters and select the Cascade check box.

For more details on the definition of new Entry Queues refer to the MGC Manager User's Guide, Volume II, Chapter 1, Ad Hoc Auto Cascading and Cascading Links.

4 Click OK.

Creating the Dial-out Link between the Conference Running on the MGC and the Conference Running on the Collaboration Server

If the dialing is done from the MGC to the Collaboration Server, you need to define the cascaded link (dial-out participant) in the conference running on the MGC.

The dial-out string defined for the participant is the dialing string required to connect to the destination conference via the Cascade-enabled Entry Queue defined on the Collaboration Server hosting the destination cascaded conference. The dial-out participant can be defined on the MGC as template or assigned to the Meeting Room.

In the MGC Manager application, define a new participant as follows:

- 1 In the Participant Properties Identification dialog box, enter a Participant Name
- 2 In the Connection Type field, select Dial-out.
- 3 In the Interface Type list field, select H.323.
- **4** There are two methods to define the dialing string to the other conference:
 - a Using the MCU's IP Address and the Alias string Method A

b Using only the Alias string (requires a gatekeeper) - Method B

Method A

This method does not use any gatekeepers.

In the **IP Address** field, enter the IP address of the **Signaling Host** of the Collaboration Server hosting the destination conference.

In the **Alias Name/Type** field, enter the ID of the cascade-enabled Entry Queue (EQ), the Conference ID and Password of the destination conference as follows:

<EQ ID>##<Destination Conference ID>##<Password> (Password is optional).

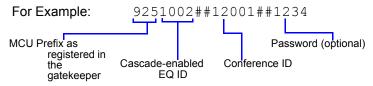


Method B

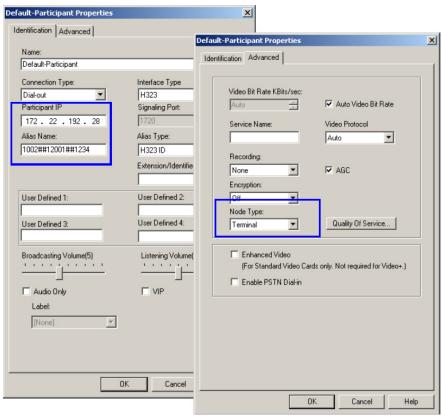
This method uses a gatekeeper.

In the **Alias Name** field, enter the Prefix of MCU B, EQ ID, Destination Conference ID, and Password, as follows:

<MCU Prefix EQ ID>##<Conference ID>##<Password> (Password is optional)



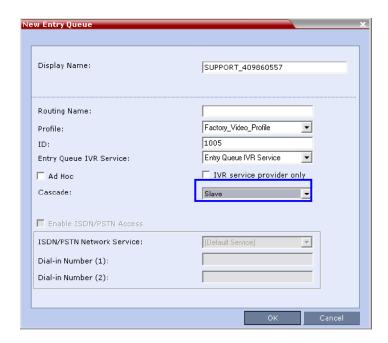
5 Click the Advanced tab and in the Node Type field, select Terminal.



6 Click OK.

Defining the Cascade Enabled Entry Queue on the Collaboration Server

If the dialing is done from the conference running on the MGC that is the Master MCU, a Cascade-enabled Entry Queue must be defined on the Collaboration Server setting it as **Slave**.



For more details, see MGC to Collaboration Server Cascading.

Defining the Cascading Conferences

The table below lists the line rates and the video settings that should be used when defining the conferences on the MGC. The same line rates should be selected when defining the Conference Profiles on the Collaboration Server, as well as whether the conference is HD Video Switching. However, the video settings will be automatically selected by the system.

Recommended Conference Line Rates for Cascaded Conferences

Topology	Video Session Mode	Conference Line Rate
MGC ↓	MGC - CIF 263 Collaboration Server - CIF 264 CP	768Kb/s, 2Mb/s
Collaboration Server	MGC - HD VSW Collaboration Server - HD VSW	1.5Mb/s

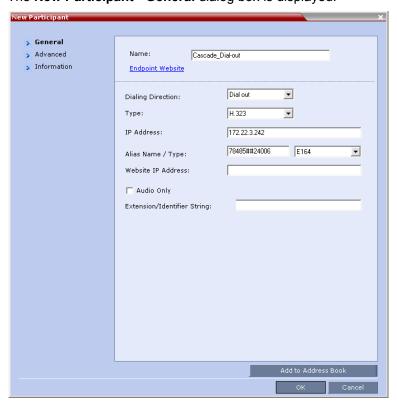
In addition, the conference running on the MGC should be set as **Meet Me Per Conference** and select the **H.239** option in the **Dual Stream Mode** field. For more details on conference definition on the MGC, refer to the *MGC Manager User's Guide, Volume I, Chapter 5*.

Defining the Dial-out Participant on the Collaboration Server

If the dialing is done from a conference running on the Collaboration Server to the conference running on the MGC, the dial-out participant is defined in the conference running on the Collaboration Server, setting the **Cascade** field to **Slave**. This participant dials the Cascade-enabled Entry Queue defined on the MGC.

1 Display the list of participants in the linked conference (Slave conference).

2 In the Participant List pane, click the New Participant () button.
The New Participant - General dialog box is displayed.



- 3 In the **Name** field, enter a participant name.
- 4 In the Dialing Direction field, select Dial-out.
- 5 In the **Type** list field, verify that **H.323** is selected.
- **6** There are two methods to define the dialing string:
 - a Using the MCU's IP Address and the Alias string Method A
 - **b** Using only the Alias string (requires a gatekeeper) Method B

Method A

This method does not used a gatekeeper.

In the **IP Address** field, enter the IP address of the MGC hosting the destination conference (Master conference).

In the **Alias Name/Type** field, enter the ID of the cascade-enabled Entry Queue (EQ), the Conference ID and Password of the destination conference (Master Conference) as follows:

<EQ ID>##<Destination Conference ID>##<Password> (Password is optional).

For Example: 1005##20006##1234

Cascade-enabled Destination Password (optional)

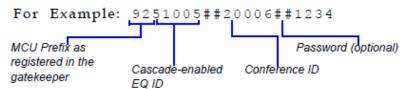
EQ ID Conference ID

Method B

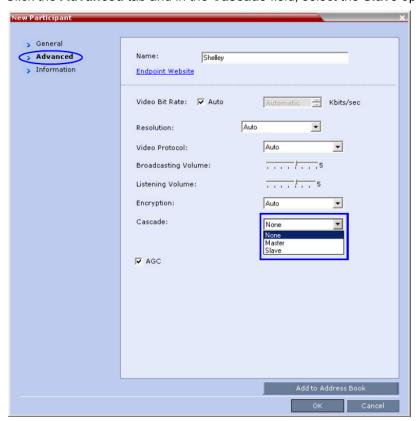
This method uses a gatekeeper.

In the **Alias Name** field, enter the MGC Prefix as registered in the gatekeeper, EQ ID, Destination Conference ID, and Password, as follows:

<MGC Prefix EQ ID>##<Conference ID>##<Password> (Password is optional)



7 Click the Advanced tab and in the Cascade field, select the Slave option.



8 Click OK.

The cascade-enabled dial-out link is created and the system automatically dials out to connect the participant to the local conference, as well as the destination conference on the MGC.

Meeting Rooms

A Meeting Room is a conference saved on the MCU in passive mode, without using any of the system resources. A Meeting Room is automatically activated when the first participant dials into it. Meeting Rooms can be activated as many times as required. Once activated, a Meeting Room functions as any ongoing conference.

The conferencing Mode of the Meeting Room is determined by the Profile assigned to it.

In SVC Conferencing Mode, dial-in is available as follows:

- AVC-capable endpoints (participants) can only connect to an AVC CP Meeting Room. When dialing
 into SVC Only Meeting Room the calls fail.
- SVC-capable endpoints support both AVC and SVC video protocols. When dialing into SVC Only
 conferences, they connect as SVC endpoints. When dialing into AVC CP Only conferences, they
 connect as AVC endpoints.
- Both AVC and SVC endpoints can connect to a mixed CP and SVC conference.

In AVC Conferencing Mode, ISDN/PSTN participants can dial-in directly to a Meeting Room without connection through an Entry Queue. Up to two numbers can be defined per conference provided that they are from the same ISDN/PSTN Network Service. When a dial-in number is allocated to a Meeting Room, the number cannot be deleted nor can the ISDN/PSTN Network Service be removed. The dial-in number must be communicated to the ISDN or PSTN dial-in participants.



ISDN participants are not supported with Collaboration Server 1800.

In AVC CP Conferences, dial-out participants can be connected to the conference automatically, or manually. In the automatic mode the system calls all the participants one after the other. In the manual mode, the Collaboration Server user or meeting organizer instructs the conferencing system to call the participant. Dial-out participants must be defined (mainly their name and telephone number) and added to the conference. This mode can only be selected at the conference/Meeting Room definition stage and cannot be changed once the conference is ongoing.

A Meeting Room can be designated as a Permanent Conference.

For more information see Audio Algorithm Support.

The maximum of number of Meeting Rooms that can be defined is:

- RealPresence Collaboration Server (RMX) 1500/1800/2000 1000
- RealPresence Collaboration Server (RMX) 4000 2000

The system is shipped with four default Meeting Rooms:

Default Meeting Rooms List

Meeting Room Name	ID	Default Line Rate
Maple_Room	1001	384 Kbps
Oak_Room	1002	384 Kbps
Juniper_Room	1003	384 Kbps
Fig_Room	1004	384 Kbps

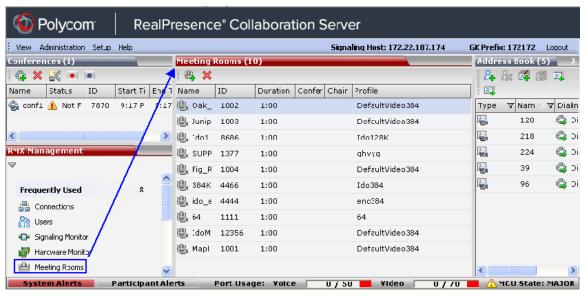
Meeting Rooms List

Meeting Rooms are listed in the **Meeting Room** list pane.

To list Meeting Rooms:

» In the RMX Management pane, in the Frequently Used list, click the Meeting Rooms button .

The Meeting Rooms list is displayed.



An active Meeting Room becomes an ongoing conference and is monitored in the same way as any other conference.

The **Meeting Room** List columns include:

Meeting Rooms List Columns

Field	Description		
Display Name	Displays the name and the icon of the Meeting Room in the Collaboration Server Web Client.		e Collaboration Server Web
An active video Meeting Room that was activated who participant connected to it.		activated when the first	
	(gray)	A passive video Meeting Room that is w	raiting to be activated.
Routing Name	The ASCII name that registers conferences, Meeting Rooms, Entry Queues and SIP Factories in the various gatekeepers and SIP Servers. In addition, the Routing Name is also: The name that endpoints use to connect to conferences. The name used by all conferencing devices to connect to conferences that must be registered with the gatekeeper and SIP Servers.		
ID	Displays the Meeting Room ID. This number must be communicated to H.323 conference participants to enable them to dial in.		
Duration	Displays the duration of the Meeting Room in hours using the format HH:MM (default 01:00).		
Conference Password	The password to be used by participants to access the Meeting Room. If blank, no password is assigned to the conference. This password is valid only in conferences that are configured to prompt for a conference password in the IVR Service. The Collaboration Server can be configured to automatically generate conference and chairperson passwords		
Chairperson Password	Displays the password to be used by the users to identify themselves as Chairpersons. They are granted additional privileges. If left blank, no chairperson password is assigned to the conference. This password is valid only in conferences that are configured to prompt for a chairperson password.		
Profile	Displays the name of the Profile assigned to the Meeting Room. For more information, see Defining New Profiles.		

Meeting Rooms List Columns (Continued)

Field	Description	
SIP Registration	 The status of registration with the SIP server: Not configured - Registration with the SIP Server was not enabled in the Conference Profile assigned to this conferencing Entity. In Multiple Networks configuration, If one service is not configured while others are configured and registered, the status reflects the registration with the configured Network Services. The registration status with each SIP Server can be viewed in the Properties - Network Services dialog box of each conferencing entity. When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register with a URL derived from its own signaling address. In Collaboration Server 1500/2000/4000, this unique URL replaces the non-unique URL, dummy_tester, used in previous versions. Failed - Registration with the SIP Server failed. This may be due to incorrect definition of the SIP server in the IP Network Service, or the SIP server may be down, or any other reason the affects the connection between the Collaboration Server or the SIP Server to the network. 	
	 Registered - the conferencing entity is registered with the SIP Server. Partially Registered - This status is available only in Multiple Networks configuration, when the conferencing entity failed to register to all the required Network Services if more than one Network Service was selected. 	

Meeting Room Toolbar & Right-click Menu

The Meeting Room toolbar and right-click menus provide the following functionality:

Meeting Room Toolbar and Right-click Menus

Toolbar button	Right-click menu	Description
	New Meeting Room	Select this button to create a new Meeting Room.
×	Delete Meeting Room	Select any Meeting Room and then click this button to delete the Meeting Room.



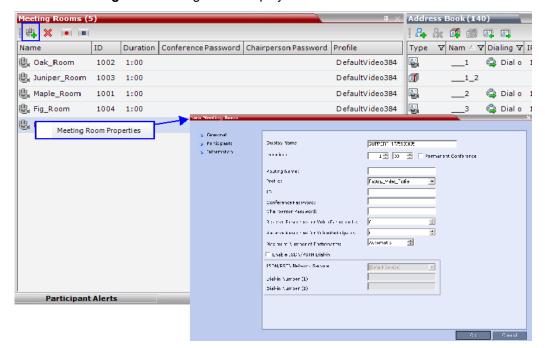
Dial out to AVC participants assigned to a Meeting Room will only start when the dial in participant who has activated it has completed the connection process and the Meeting Room has become an ongoing conference.

Creating a New Meeting Room

To create a new meeting room:

• In the **Meeting Rooms** pane, click the **New Meeting Room** button or right-click an empty area in the pane and then click **New Meeting Room**.

The **New Meeting Room** dialog box is displayed.



The definition procedure is the same as for the new conference (with the exception of Reserved Resources for Audio and Video participants in the Collaboration Server 1500/2000/4000 only).



If SIP Factories are being used do not assign a Meeting Room the ID 7001. This ID is reserved for the default SIP Factory.

For more information, see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, Starting an AVC CP Conference from the Conferences Pane. Microsoft Lync users can connect a Collaboration Server Meeting Room to a conference running on the Microsoft A/V MCU. This allows Collaboration Server Lync users to connect with a conference in progress on the A/V MCU and be an active participant in the conference.

For more information, see Connecting a Collaboration Server Meeting Room to a Microsoft AV-MCU Conference.

Entry Queues, Ad Hoc Conferences and SIP Factories

Entry Queues

An Entry Queue (EQ) is a special routing lobby to access conferences. Participants connect to a single-dial lobby and are routed to their destination conference according to the Conference ID they enter. The Entry Queue remains in a passive state when there are no callers in the queue (in between connections) and is automatically activated once a caller dials its dial-in number.

Participants can be moved from the Entry Queue and the destination conference if both conferencing entities are set to the same conferencing parameters: Conferencing Mode, Line rate and video parameters. For example, participants can be moved from SVC Only Entry Queue to SVC Only conference, or from a mixed CP and SVC Entry Queue to a mix CP and SVC conference, from CP only Entry Queue to CP only conference.

The maximum of number of Entry Queues that can be defined is:

- RealPresence Collaboration Server (RMX) 1500/1800/2000 40
- RealPresence Collaboration Server (RMX) 4000 80

The parameters (bit rate and video properties) with which the participants connect to the Entry Queue and later to their destination conference are defined in the Conference Profile that is assigned to the Entry Queue. For example, if the Profile Bit Rate is set to 384kbps, all endpoints connect to the Entry Queue and later to their destination conference using this bit rate even if they are capable of connecting at higher bit rates.

An Entry Queue IVR Service must be assigned to the Entry Queue to enable the voice prompts guiding the participants through the connection process. The Entry Queue IVR Service also includes a video slide that is displayed to the participants while staying in the Entry Queue (during their connection process).

Different Entry Queues can be created to accommodate different conferencing modes, conferencing parameters (by assigning different Profiles) and prompts in different languages (by assigning different Entry Queue IVR Services).

For more information, see IVR Services List.

The Entry Queue can also be used for Ad Hoc conferencing. If the Ad Hoc option is enabled for the Entry Queue, when the participant enters the target conference ID the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID. For more information about Ad Hoc conferencing, see Ad Hoc Conferencing.

An Entry Queue can be designated as Transit Entry Queue to which calls with dial strings containing incomplete or incorrect conference routing information are transferred. For more information, see Transit Entry Queue.

To enable ISDN/PSTN participants to dial in to the Entry Queue, an ISDN/PSTN dial-in number must be assigned to the Entry Queue. Up to two dial-in numbers can be assigned to each Entry Queue. The dial-in numbers must be allocated from the dial-in number range defined in the ISDN/PSTN Network Service. You can allocate the two dial-in numbers from the same ISDN/PSTN Network Service or from two different ISDN/PSTN Network Services. The dial-in number must be communicated to the ISDN or PSTN dial-in participants.



Collaboration Server 1800 does not support:

- · ISDN connections
- · Video Switching Conferencing Mode

The Entry Queue can also be used as part of the Gateway to Polycom® RealPresence DMA solution for connecting Audio only PSTN, ISDN, SIP and H.323 endpoints to RealPresence DMA™ system.

For more information, see Dialing to Polycom® RealPresence DMA System.

Default Entry Queue properties

The system is shipped with a default Entry Queue whose properties are shown in the following table.

Default Entry Queue Properties

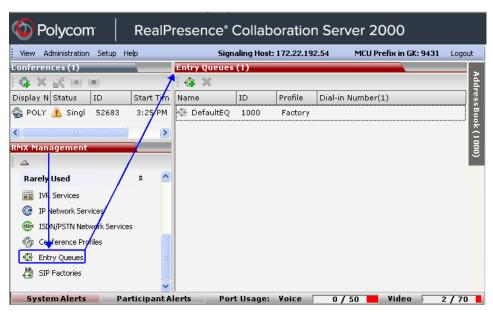
Parameter	Value	
Display Name	DefaultEQ	
	The user can change the name if required.	
Routing Name	DefaultEQ	
	The default Routing Name cannot be changed.	
ID	1000	
Profile name	Factory_Video_Profile. Profile Bit Rate is set to 384 Kbps.	
Entry Queue Service	Entry Queue IVR Service. This is default Entry Queue IVR Service shipped with the system and includes default voice messages and prompts in English.	
Ad Hoc	Enabled	
Cascade	None (Disabled)	
Enable ISDN/PSTN Access	Disabled. You can modify the properties of this Entry Queue to enable ISDN/PSTN participants to dial-in to a conference. Up to two dial-in numbers can be assigned.	

Defining a New Entry Queue

You can modify the properties of the default Entry Queue and define additional Entry Queues to suit different conferencing requirements.

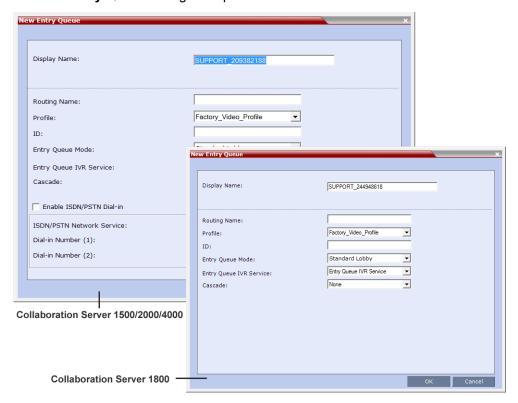
To define a new Entry Queue:

1 In the RMX Management pane, In the Rarely Used menu, click Entry Queues.



2 In the Entry Queues list pane, click the New Entry Queue button.

The New Entry Queue dialog box opens.



3 Define the following parameters:

Entry Queue Definitions Parameters

Option	Description
Display Name	 The Display Name is the conferencing entity name in native language character sets to be displayed in the Collaboration Server Web Client. In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the Display Name field that can be modified using Unicode encoding. English text uses ASCII encoding and can contain the most characters (length varies according to the field). European and Latin text length is approximately half the length of the maximum. Asian text length is approximately one third of the length of the maximum. The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII). Maximum field length in ASCII is 80 characters. If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message requesting you to enter a different name.
Routing Name	 Enter a name using ASCII text only. If no Routing Name is entered, the system automatically assigns a new name as follows: If an all ASCII text is entered in Display Name, it is used also as the Routing Name. If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.
Profile	Select the Profile to be used by the Entry Queue. The default Profile is selected by default. This Profile determines the Bit Rate and the video properties with which participants connect to the Entry Queue and destination conference. To connect to a Video Switching conference via Entry Queue, the Profile assigned to the Entry Queue must be set to Video Switching. It is recommended to use the same profile for both the destination conference and Entry Queue. In Ad Hoc conferencing, it is used to define the new conference properties.
ID	Enter a unique number identifying this conferencing entity for dial in. Default string length is 4 digits. If you do not manually assign the ID, the MCU assigns one after the completion of the definition. The ID String Length is defined by the flag NUMERIC_CONF_ID_LEN in the System Configuration.

Entry Queue Definitions Parameters

Option	Description
Entry Queue Mode	Select the mode for the Entry Queue
	Standard Lobby (default) - When selected, the Entry Queue is used as a routing lobby to access conferences. Participants connect to a single-dial lobby and are routed to their destination conference according to the Conference ID they enter.
	Ad Hoc - Select this option to enable the Ad Hoc option for this Entry Queue. In this mode, when the participant enters the target conference ID the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID.
	IVR Only Service Provider - When selected, designates this Entry Queue as a special Entry Queue that provides IVR Services to SIP calls on behalf of the RealPresence DMA system. The IVR Only Service Provider Entry Queue does not route the SIP calls to a target conference. Instead the RealPresence DMA system handles the call. For more details, see IVR Provider Entry Queue (Shared Number Dialing).
	External IVR Control - IVR Services can be controlled externally from an application server (such as the DMA) supporting the MCCF-IVR (Media Control Channel Framework-Interactive Voice Response) package. When selected, the connection process of the participant to the conference via the Virtual Entry Queue is controlled and managed by an external IVR service of an application server (for example, DMA).
Entry Queue IVR Service	The default Entry Queue IVR Service is selected. If required, select an alternate Entry Queue IVR Service, which includes the required voice prompts, to guide participants during their connection to the Entry Queue.
Cascade	 Set this field to None for all Entry Queues other than cascading. If this Entry Queue is used to connect dial-in cascaded links, select Master or Slave depending on the Master/Slave relationship in the Cascading topology. Set this field to Master if: The Entry Queue is defined on the MCU on level 1 and the dialing is done from level 2 to level 1. The Entry Queue is defined on the MCU on level 2 and the dialing is done from level 3 to level 2. Set this field to Slave if the Entry Queue is defined on the MCU on level 2 (Slave) and the dialing is done from MCU level 1 to level 2.
Enable ISDN/PSTN Access	Select this check box to allocate dial-in numbers for ISDN/PSTN connections. To define the first dial-in number using the default ISDN/PSTN Network Service, leave the default selection. When the Entry Queue is saved on the MCU, the dial-in number will be automatically assigned to the Entry Queue. This number is taken from the dial-in numbers range in the default ISDN/PSTN Network Service.
ISDN/PSTN Network Service	The default Network Service is automatically selected. To select a different ISDN/PSTN Network Service in the service list, select the name of the Network Service.

Entry Queue Definitions Parameters

Option	Description
Dial-in Number (1)	Leave this field blank to let the system automatically assign a number from the selected ISDN/PSTN Network Service. To manually define a dial-in number, enter a required number from the dial-in number range defined for the selected Network Service.
Dial-in Number (2)	By default, the second dial-in number is not defined. To define a second-dial-in number, enter a required number from the dial-in number range defined for the selected Network Service.

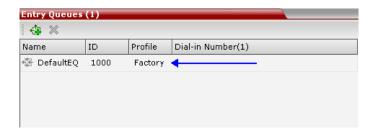
4 Click OK.

The new Entry Queue is added to the Entry Queues list.

Listing Entry Queues

To view the list of Entry Queues:

In the RMX Management pane- Rarely Used menu, click Entry Queues.
 The Entry Queues are listed in the Entry Queues pane.



You can double-click an Entry Queue to view its properties.

Modifying the EQ Properties

To modify the EQ:

• In the **Entry Queues** pane, either double-click or right-click, and select **Entry Queue Properties** of the selected Entry Queue in the list.

The **Entry Queue Properties** dialog box is displayed. All the fields may be modified except Routing Name.

Transit Entry Queue

A Transit Entry Queue is an Entry Queue to which calls with dial strings containing incomplete or incorrect conference routing information are transferred.

IP Calls are routed to the Transit Entry Queue when:

- A gatekeeper is not used, or where calls are made directly to the Collaboration Server's Signaling IP Address, with incorrect or without a Conference ID.
- When a gatekeeper is used and only the prefix of the Collaboration Server is dialed, with incorrect or without a Conference ID.
- When the dialed prefix is followed by an incorrect conference ID.

When no Transit Entry Queue is defined, all calls containing incomplete or incorrect conference routing information are rejected by the Collaboration Server.

In the Transit Entry Queue, the Entry Queue IVR Service prompts the participant for a destination conference ID. Once the correct information is entered, the participant is transferred to the destination conference.

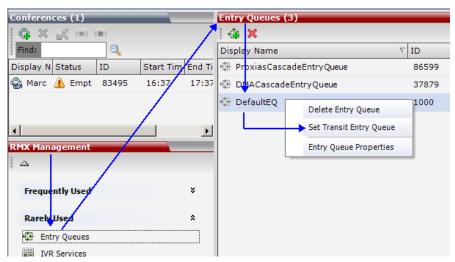
Setting a Transit Entry Queue

The Collaboration Server factory default settings define the Default Entry Queue also as the Transit Entry Queue. You can designate another Entry Queue as the Transit Entry Queue.

Only one Transit Entry Queue may be defined per Collaboration Server and selecting another Entry Queue as the Transit Entry Queue automatically cancels the previous selection.

To designate an Entry Queue as Transit Entry Queue:

- 1 In the RMX Management pane, Rarely Used list, click Entry Queues.
- 2 In the Entry Queues list, right-click the Entry Queue entry, and then click Set Transit Entry Queue.



The Entry Queue selected as Transit Entry Queue is displayed in bold.

To cancel the Transit Entry Queue setting:

- 1 In the RMX Management pane, Rarely Used list, click Entry Queues.
- 2 In the Entry Queues list, right-click the Transit Entry Queue entry, and then click Cancel Transit Entry Queue.

IVR Provider Entry Queue (Shared Number Dialing)

In an environment that includes a RealPresence DMA system, the Collaboration Server Entry Queue can be configured to provide the IVR Services on behalf of the RealPresence DMA system to SIP endpoints. It displays the Welcome Slide, plays the welcome message and retrieves the destination conference ID that is entered by the participant using DTMF codes.

To enable this feature, a special Entry Queue that is defined as IVR Only Service Provider is created. This Entry Queue does not forward calls to conferences running on the Collaboration Server and its main functionality is to provide IVR services.

Call Flow

The SIP participant dials the DMA Virtual Entry Queue number, for example 1000@dma.polycom.com.

The DMA forwards the SIP call to the Collaboration Server, to a special Entry Queue that is configured as IVR Only Service Provider. The participant is prompted to enter the conference ID using DTMF codes.

Once the participant enters the conference ID, the conference ID is forwarded to the DMA, enabling the DMA to connect the SIP endpoint to the destination conference or create a new conference and connect the participant to that conference.

Guidelines for setting the Entry Queue as IVR Provider

- An Entry Queue defined as IVR Only Service Provider does not route the SIP call to a target conference and it cannot be used to route calls on the Collaboration Server. In such a configuration, the DMA handles the calls. Therefore, normal Entry Queues must be defined separately.
- Operator Assistance must be disabled in the IVR Service assigned to this Entry Queue.
- Only the conference ID prompts should be configured. Other prompts are not supported in IVR Only Service Provider configuration.
- PSTN, ISDN, H.323 calls to this Entry Queue are rejected.
- The DMA must be configured to locate the IVR Only Service Provider Entry Queue on the Collaboration Server. To locate the Entry Queue the DMA requires the Entry Queue's ID number and the Collaboration Server Signaling IP address (xxx.xxx.xxx).

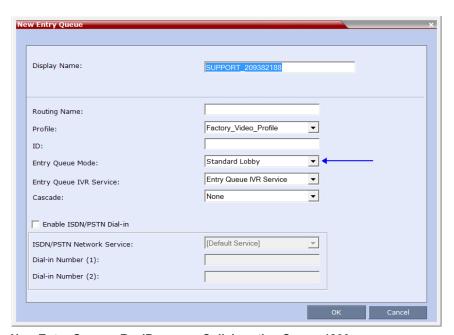
Configuring the Collaboration Server as IVR Provider

Entry Queue IVR Service

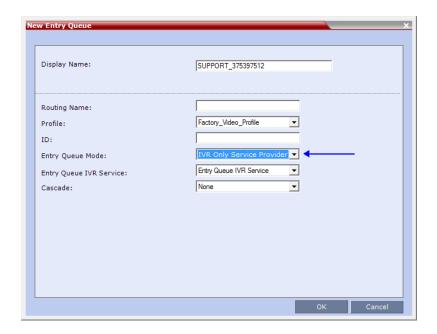
If required, create a special Entry Queue IVR Service in which the **Operator Assistance** option is disabled, and only the Conference ID prompts are enabled.

Entry Queue

» In the New Entry Queue dialog box, Entry Queue Mode list, select IVR Only Service Provider.
New Entry Queue - RealPresence Collaboration Server (RMX) 1500/2000/4000



New Entry Queue - RealPresence Collaboration Server 1800



- > Enter the Entry Queue ID to be used by the DMA for forwarding the SIP calls to this Entry Queue.
- > Select the special **Entry Queue IVR Service** if one was created.

The Cascade and Enable ISDN/PSTN Dial-in options should not be enabled with this type of Entry Queue.

Using External IVR Services via the MCCF-IVR Package

IVR Services can be controlled externally from an application server supporting the MCCF-IVR (Media Control Channel Framework-Interactive Voice Response) package. The external IVR service is currently being implemented with the integration of the Polycom RealPresence Virtualization Manager (DMA) as the application server. When the application server is deployed in the enterprise environment and the Polycom RealPresence Collaboration Server (MCU) is deployed as a media server, the external IVR service can be used to play audio messages, display slides, and collect DTMF input from the participant. The external IVR service is managed by the application server at the pre-conference phase when the participant is placed into a special external IVR-controlled Entry Queue in the Collaboration Server (MCU), collecting information before connecting to the conference.

The external IVR-controlled Entry Queue plays recorded voice messages or sends video slides such as splash screens to the participant and collects DTMF input from the participant such as conference ID and conference password for various functions.

IVR media files, WAV for voice messages and JPG for video slides, are stored on the application server. In order to provide external IVR control, a TCP-based MCCF channel is created between the application server and the media server. Because of real-time considerations, when the MCCF channel is established, the application server notifies the media server about the media files. The media server downloads the media files. The media server is notified by the application server when to download new or updated media files.

When the call has completed the pre-conference phase in the external IVR-controlled Entry Queue, the application server disconnects the call from the Entry Queue and routes the call to an ongoing conference or creates a new VMR.

Call Flows

The external IVR-controlled Entry Queue can be initiated for various types of calls from SIP endpoints such as standalone endpoints and Cisco TIP endpoints. Standalone endpoints are SIP or H.264 TIP endpoints. These endpoints can include HDX systems, multiple Telepresence (ITP) screens, and RealPresence Desktop client applications.

Call Flow for Standalone SIP Endpoints

The following describes how a standalone SIP endpoint call is placed into the IVR-controlled Entry Queue and is then connected to a conference:

- 1 A SIP call is routed through the application server to the IVR-controlled Entry Queue.
- 2 The MCU answers the call and waits for the IVR media file requests from the application server. The MCU does not control the call while the call is in the Entry Queue.
- 3 The application server may request, through the MCCF channel IVR package, to play an audio file and display a slide. When the audio file has finished playing, the MCU notifies the application server that the audio file has been played for the call.
- 4 The application server may request, through the MCCF channel IVR package, to collect DTMF input such as a conference ID or password, from the caller. The DTMF input is transferred from the MCU to the application server. When the application server receives the DTMF input, it validates the

- input for the required conference ID or password. If the input is incorrect, the application server will request the MCU to replay the audio file and collect the DTMF input again. The MCU transfers the DTMF input to the application server for revalidation.
- 5 When the application server has completed the pre-conference IVR, the application server routes the call to a VMR with the collected password appended to the following dial string:

```
<conf-id>**<password>@mcu-sig-ip.
```

- The call is disconnected from the application server. The MCU now has control of the call.
- **6** The call is transferred to a conference, which can reside on another MCU.

Call Flow for Standalone TIP Endpoints

The following describes how a standalone TIP endpoint call is placed into the IVR-controlled Entry Queue and is then connected to a conference:

- 1 A TIP call is routed through the application server to the IVR-controlled Entry Queue. TIP endpoints can either have a single screen or multiple screens.
- 2 The MCU answers the call and waits for the IVR media file requests from the application server. The MCU does not control the call while the call is in the Entry Queue.
- 3 The application server may request, through the MCCF channel IVR package, to play an audio file and display a video slide. When the TIP endpoint uses multiple screens, the video slide is displayed on the main screen only. When the audio file has finished playing, the MCU notifies the application server that the audio file has been played for the call.
- 4 The application server may request, through the MCCF channel IVR package, to collect DTMF input such as a conference ID or password, from the caller. When the TIP endpoint uses multiple screens, the DTMF input is collected only once from the main screen. The DTMF input is transferred from the MCU to the application server. When the application server receives the DTMF input, it validates the input for the required conference ID or password. Because TIP uses DTLS, it can optionally enable re-keying of DTMF input and the calls to the Entry Queue and the conference can be encrypted.
- 5 When the application server has completed the pre-conference IVR, the application server routes the call to a VMR with the collected password appended to the following dial string:

```
<conf-id>**<password>@mcu-sig-ip.
```

The call is disconnected from the application server. The MCU now has control of the call.

6 The call is transferred to a conference, which can reside on another MCU.

Call Flow for TIP Endpoints from a Polycom ITP System

The following describes how a TIP call from Cisco TPS endpoints or TIP calls from a Polycom ITP system working as a TIP call is placed into the IVR-controlled Entry Queue and is then connected to a conference:

- 1 A TIP call is routed through the application server to the IVR-controlled Entry Queue.
- 2 The MCU answers the call and waits for the IVR media file requests from the application server. The MCU does not control the call while the call is in the Entry Queue.
- 3 While the call is in the Entry Queue, video is only displayed on the main screen.
- **4** DTMF input is collected only once from the main screen. Because TIP uses DTLS, it can optionally enable re-keying of DTMF input and the calls to the Entry Queue and the conference can be encrypted.

5 When the application server has completed the pre-conference IVR, the application server routes the call to a VMR with the collected password appended to the following dial string:

```
<conf-id>**<password>@mcu-siq-ip. The MCU now has control of the call.
```

The call is transferred to a conference, which can reside on another MCU.

Guidelines for Using External IVR Services via the MCCF-IVR Package

- AVC SIP and TIP protocols are supported in the RealPresence Collaboration Server 1500/2000/4000 only.
- MCCF channels support both IPV4 and IPV6.
- When the MCCF channel is disconnected, an alarm is displayed and all external IVR files are deleted. When the MCCF channel is reconnected, the external IVR files are sent to the MCU.
- When the Collaboration Server (MCU) is restarted, all existing external IVR files are deleted. When
 the MCCF channel connects to the Collaboration Server, the external IVR file are sent to the
 Collaboration Server.
- H.323 and ISDN protocols are not supported.
- In Collaboration Server 1500/2000/4000 only, Video Switching conferences do not support the TIP protocol
- TIP-based conferencing does not support the following features during conferences:
 - Gathering phase
 - > Skin display
 - Text messaging using Message Overlay
 - Site Name display
 - > PCM
 - Click&View
- To play audio messages and display the welcome slide during the participant connection to the conference via the Virtual Entry Queue, the Media files have to meet the following requirements (as defined in the Entry Queue IVR Service):
 - Audio messages: WAV files PCM, 16 KHz, 16 bit, Mono
 - Video slides: JPG files 1920 x 1088 resolution

Configuring the MCU to Support External IVR Services via the MCCF-IVR

The support of External IVR Services via the MCCF-IVR package is enabled by default in the Collaboration Server (RMX) systems, by the flag **ENABLE_MCCF** which is set to **YES**.

However, in Ultra Secure Mode and in secured environments where the External IVR Services via the MCCF-IVR package is not required and unused ports should be closed, this flag should be set to **NO**.

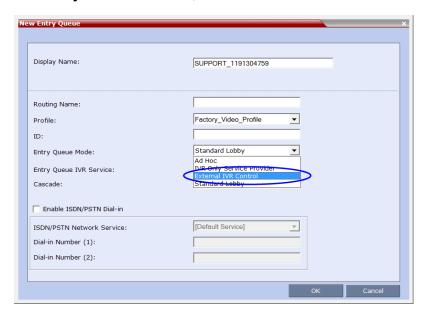
To change this flag value from YES to No, you must first add it to the System Configuration. For more details, see Manually Adding and Deleting System Flags.

Configuring the Entry Queue to Use External IVR Services

The Entry Queue can be configured to place a call in the external IVR-controlled Entry Queue.

To configure the Entry Queue for External IVR Services:

- 1 In the RMX Management pane, click Entry Queues.
- 2 In the Entry Queues pane, click the New Entry Queue icon.
 The New Entry Queue dialog box is displayed.
- 3 In the Display Name field, type an appropriate display name for the Entry Queue.
- 4 In the Entry Queue Mode field, select External IVR Control from the available options.



When **External IVR Control** is selected, the connection process of the participant to the conference via the Virtual Entry Queue is controlled and managed by an external IVR service of an application server (for example, DMA).

5 Click OK.

SIP Factories

A SIP Factory is a conferencing entity that enables SIP endpoints to create Ad Hoc conferences. The system is shipped with a default SIP Factory, named **DefaultFactory**.



The default SIP Factory uses the conferencing ID 7001. If a SIP Factory is being used do not assign this ID to any conferencing entity, including conferences, reservations, and meeting rooms.

When a SIP endpoint calls the SIP Factory URI, a new conference is automatically created based on the Profile parameters, and the endpoint joins the conference.

The SIP Factory URI must be registered with the SIP server to enable routing of calls to the SIP Factory. To ensure that the SIP factory is registered, the option to register **Factories** must be selected in the Default IP Network Service.

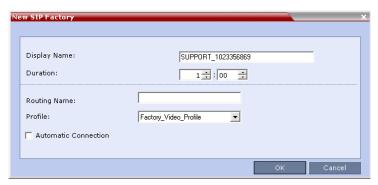
The maximum of number of SIP Factories that can be defined is 40.

Creating SIP Factories

To create a new SIP Factory:

- 1 In the RMX Management pane, Rarely Used list, click SIP Factories.
- ${\bf 2}$ $\,$ In the SIP Factories list pane, click the New SIP Factory button.

The **New Factory** dialog box opens.



3 Define the following parameters:

New Factory Properties

Option	Description
Display Name	Enter the SIP Factory name that will be displayed.
	The Display Name is the conferencing entity name in native language character sets to be displayed in the Collaboration Server Web Client.
	In conferences, Meeting Rooms, Entry Queues and SIP factories the system automatically generates an ASCII name for the Display Name field that can be modified using Unicode encoding.
	 English text uses ASCII encoding and can contain the most characters (length varies according to the field).
	 European and Latin text length is approximately half the length of the maximum.
	 Asian text length is approximately one third of the length of the maximum.
	The maximum length of text fields also varies according to the mixture of character sets (Unicode and ASCII).
	Maximum field length in ASCII is 80 characters. If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message requesting you to enter a different name.
Routing Name	The Routing Name is defined by the user, however if no Routing Name is entered, the system will automatically assign a new name when the Profile is saved as follows:
	 If an all ASCII text is entered in Display Name, it is used also as the Routing Name.
	 If any combination of Unicode and ASCII text (or full Unicode text) is entered in Display Name, the ID (such as Conference ID) is used as the Routing Name.

New Factory Properties

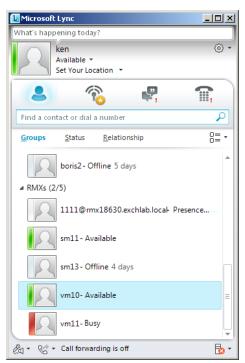
Option	Description
Profile	The default Profile is selected by default. If required, select the conference Profile from the list of Profiles defined in the MCU. A new conference is created using the parameters defined in the Profile.
Automatic Connection	Select this check box to immediately accept the conference creator endpoint to the conference. If the check box is cleared, the endpoint is redirected to the conference and then connected.

4 Click OK.

The new SIP Factory is added to the list.

SIP Registration & Presence for Entry Queues and SIP Factories with SIP Servers

Entry Queues and SIP Factories can be registered with SIP servers. This enables Office Communication Server or Lync server client users to see the availability status (**Available**, **Offline**, or **Busy**) of these conferencing entities, and to connect to them directly from the Buddy List.



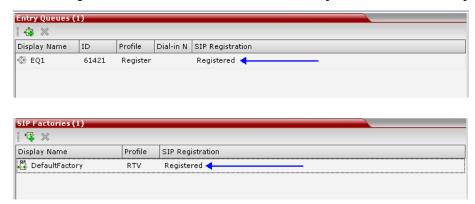
Guidelines for registering Entry Queues and SIP Factories with SIP Servers

• The Entry Queue or SIP Factory must be added to the Active Directory as a User.

 SIP Registration must be enabled in the Profile assigned to the Entry Queue or SIP Factory. For more information see Defining New Profiles.

Monitoring Registration Status

The SIP registration status can be viewed in the Entry Queue or SIP Factory list panes.



The following statuses are displayed:

 Not configured - Registration with the SIP Server was not enabled in the Conference Profile assigned to the Entry Queue or SIP Factory.

When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register with an URL derived from its own signaling address. In Collaboration Server 1500/2000/4000, this unique URL replaces the non-unique URL, dummy_tester, used in previous versions.

Failed - Registration with the SIP Server failed.

This may be due to incorrect definition of the SIP server in the IP Network Service, or the SIP Server may be down, or any other reason the affects the connection between the Collaboration Server or the SIP Server to the network.

- Registered The conferencing entity is registered with the SIP Server.
- Partially Registered This status is available only in Multiple Networks configuration, when the
 conferencing entity failed to register to all the required Network Services, if more than one Network
 Service was selected for Registration.

Ad Hoc Conferencing

The Entry Queue can also be used for Ad Hoc conferencing. If the **Ad Hoc** option is enabled for the Entry Queue, when the participant enters the target conference ID the system checks whether a conference with that ID is already running on the MCU. If not, the system automatically creates a new ongoing conference with that ID. The conference parameters are based on the Profile linked to the Entry Queue. As opposed to Meeting Rooms, that are predefined conferences saved on the MCU, Ad Hoc conferences are not stored on the MCU. Once an Ad Hoc conference is started, it becomes an ongoing conference, and is monitored and controlled as any standard ongoing conference.

An external database application can be used for authentication with Ad Hoc conferences. The authentication can be done at the Entry Queue level and at the conference level. At the Entry Queue level, the MCU queries the external database server whether the participant has the right to create a new

conference. At the conference level the MCU verifies whether the participant can join the conference and if the participant is the conference chairperson. The external database can populate certain conference parameters.

For more information about Ad Hoc conferencing, see Appendix D - Ad Hoc Conferencing and External Database Authentication.

Gateway to Polycom® Distributed Media Application™ (DMA™) 7000 (Collaboration Server 1500/2000/4000 only)



ISDN participants are not supported with Collaboration Server 1800.

Gateway to Polycom® Distributed Media Application™ (DMA™) 7000 enables audio only PSTN, ISDN (video endpoints using only their audio channels), SIP and H.323 calls to connect to the Polycom DMA 7000 via gateway sessions running on the Collaboration Server. Each Collaboration Server conference acting as a gateway session includes one connection to the endpoint and another connection to the DMA. The DMA 7000 enables load balancing and the distribution of multipoint calls on up to 10 Polycom Collaboration Server media servers.

As part of this solution, the Collaboration Server acts as a gateway for the DMA that supports H.323 calls. The PSTN, ISDN or SIP endpoint dials the virtual Meeting Room on the DMA via a special Entry Queue on the Collaboration Server.

For more information, see Dialing to Polycom® RealPresence DMA System.

Address Book

The Address Book stores information about the people and businesses you communicate with. The Address Book stores, among many other fields, IP addresses, phone numbers and network communication protocols used by the participant's endpoint. By utilizing the Address Book you can quickly and efficiently assign or designate participants to conferences. Groups defined in the Address Book help facilitate the creation of conferences. Participants can be added to the Address Book individually or in Groups.

The maximum of number of Address Book entries that can be defined on the Collaboration Server is 4000.

When using the Polycom CMA/RealPresence Resource Manager Global Address Book, all entries are listed.

The Address Book can be organized into a multi-level hierarchical structure. It can be used to mirror the organizational layout of the enterprises and it is especially suitable for large-scale enterprises with a considerable number of conference participants and organizational departments and divisions. Groups in the Address Book can contain sub-groups or sub-trees, and individual address book participant entities.

The Address Book provides flexibility in arranging conference participants into groups in multiple levels and the capabilities to add groups or participants, move or copy participants to multiple groups within the address book, and use the address book to add groups and participants to a conference or Conference Template.

Importing and exporting of Address Books enables organizations to seamlessly distribute up-to-date Address Books to multiple Collaboration Server units. It is not possible to distribute Address Books to external databases running on applications such as Polycom's RealPresence Resource Manager or Polycom CMA. External databases can run in conjunction with Collaboration Server units, but must be managed from the external application. For example, new participants cannot be added to the external database from the Collaboration Server Web Client. To enable the Collaboration Server to run with an external database such as Polycom RealPresence Resource Manager or CMA, the appropriate system configuration flags must be set.

For more information, see Modifying System Flags.



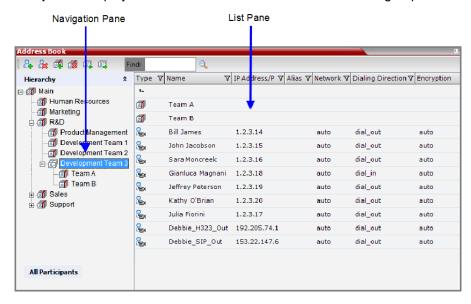
Integration with the Global Address Book of the Polycom RealPresence Resource Manager (XMA) or CMA is supported. For more information, see Integrating the Global Address Book (GAB) of Polycom RealPresence Resource Manager (XMA) or Polycom CMA™ with the Collaboration Server. Integration with the SE200 GAB (Global Address Book) is not supported.

Viewing the Address Book

You can view the participants currently defined in the Address Book. The first time the Collaboration Server Web Client is accessed, the **Address Book** pane is displayed.

The Address Book contains two panes:

- Navigation pane Contains the hierarchical tree and All Participants list.
- List pane Displays the list of all the members of the selected group and sub-groups.



The **Navigation pane** of the Address Book contains the following types of lists:

- **Hierarchical** Displays a multi-level hierarchical tree of groups and participants. Double-clicking a group on the navigation pane displays the group participants and sub-groups in the **List** pane.
- All Participants Double-clicking this selection displays the single unique entity of all the
 participants in a single level. When adding a participant to a group, the system adds a link to the
 participant's unique entity that is stored in the All Participants list. The same participant may be added
 to many groups at different levels, and all these participant links are associated with the same
 definition of the participant in the All Participants list. If the participant properties are changed in one
 group, they will be changed in all the groups accordingly.

Displaying and Hiding the Group Members in the Navigation Pane

To expand the group to view the group members:

» Double-click the group name or click the **Expand** 🛨 button.

The address book entities and sub-groups of the group is displayed in the right group list pane. You can drill down the sub-group to view address book entities in the sub-group.

To move up to the next level and view the members in the upper level:

» Double-click the **navigation arrow** button in the group members pane.

To collapse a group:

» Double-click the group name or click the **Collapse** \blacksquare button.

Participants List Pane Information

The Participants List pane displays the following information for each participant:



Participants List Pane

Field/Option	Description
Туре	Indicates whether the participant is a video ([2]) or voice ([2]).
Name	Displays the name of the participant.
IP Address/Phone	 Enter the IP address of the participant's endpoint. For H.323 participant define either the endpoint IP address or alias. For SIP participant define either the endpoint IP address or the SIP address. Note: This field is removed from the dialog box when the ISDN/PSTN protocol is selected (Collaboration Server 1500/2000/4000 only).
Network	The network communication protocol used by the endpoint to connect to the conference: H.323 or SIP or ISDN/PSTN (Collaboration Server 1500/2000/4000 only).
Dialing Direction	Dial-in – The participant dials in to the conference. Dial-out – The Collaboration Server dials out to the participant.
Encryption	Displays whether the endpoint uses encryption for its media. The default setting is Auto , indicating that the endpoint must connect according to the conference encryption setting.

For information on adding and modifying participants in the Address Book, see Managing the Address Book.

Displaying and Hiding the Address Book

The Address Book can be hidden it by clicking the anchor pin () button in the pane header. The **Address Book** pane closes and a tab is displayed at the right edge of the screen.

» Click the tab to re-open the Address Book.



Adding Participants from the Address Book to Conferences

You can add individual participants or a group of participants from the Address Book to a conference.

Adding Individual Participants from the Address Book to Conferences

You can add a participant or multiple participants to a new conference, ongoing conferences, or to **Conference Templates** by using the drag-and-drop operation.



Multiple selection of group levels is not available.

To add a participant to a new conference or an ongoing conference:

- 1 In the Address Book Navigation pane, select the group from which to add participants.
- 2 In the Address Book List pane, select the participant or participants you want to add to the conference.
- 3 Click and hold the left mouse button and drag the selection to the Participants pane of the conference.

The participants are added to the conference.

Adding a Group from the Address Book to Conferences

You can add a group of participants to a new conference, ongoing conferences, or to **Conference Templates** by using the drag-and-drop operation.

To add a group to a new conference or an ongoing conference:

- 1 In the Address Book Navigation pane, select the group you want to add to the conference.
- 2 Click and hold the left mouse button and drag the selection to the Participants pane of the conference.

The participants in the group level and all sub-levels are added to the conference.

Participant Groups

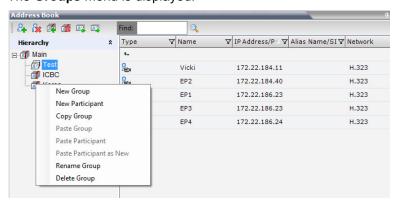
A group is a predefined collection of participants. A group provides an easy way to manage clusters of participants that are in the same organizational structure and to connect a combination of endpoints to a conference. For example, if you frequently conduct conferences with the marketing department, you can create a group called "Marketing Team" that contains the endpoints of all members of the marketing team.

Groups can contain participants and sub-groups. You can define up to ten levels in the Main group.

Managing Groups in the Address Book

To manage the groups in the Address Book:

1 In the **Address Book Navigation** pane, right-click the group you want to manage. The **Groups** menu is displayed.



2 Select one of the following actions:

Address Book Navigation

Action	Description
New Group	Creates a new group within the current group.
New Participant	Adds a new participant within the current group.
Copy Group	Copies the current group to be pasted as an additional group.
Paste Group	Places the copied group into the current group. The group name of the copied group is defined with "Copy" at the end of the group name. This action is only available after a Copy Group action has been implemented.
Paste Participant	Places the copied participant into the current selected group. This action is available after a Copy or Cut action was activated when selecting a single participant or multiple participants.
Paste Participant as New	Pastes as a new participant into the selected group. This paste action adds "Copy" at the end of the participant name. This action is only available after a Copy action was activated for a single participant.
Rename Group	Renames the group name.

Address Book Navigation (Continued)

Action	Description
Delete Group	Deletes the group and all of its members. This action displays a message requesting confirmation to delete the group and all members connected with the group.

Additionally, you can drag a group from one location in the **Address Book** to another location, moving the group and all its members, including sub-groups, to its new location using the drag-and-drop operation. Moving a group to a new location can be done in the navigation pane or the list pane.

To drag a group from a location in the address book to another location:

- 1 Select the group you want to move.
- 2 Click and hold the left mouse button and drag the selection to the new location. The new location can be either the Main root level or another group level.

The group and all its members (participants and groups) are moved to the new address book location.

Managing the Address Book

Guidelines

- The multi-level Address Book can only be used in a local configuration on the Collaboration Server. The hierarchical structure cannot be implemented with the Global Address Book (GAB).
- Up to ten levels can be defined in the hierarchical structure of the Address Book.
- The default name of the root level is Main. The Main root level cannot be deleted but the root level name can be modified.
- Address Book names support multilingual characters.
- Participants in the Address Book can be copied to multiple groups. However, only one participant
 exists in the Address Book. Groups that contain the same participants refer to the same definition of
 the participant entity.

Adding a Participant to the Address Book

Adding participants to the Address Book can be performed by the following methods:

- Directly in the Address Book.
- Moving or saving a participant from an ongoing conference to the Address Book.

Only defined **dial-out** ISDN/PSTN participants can be added to the Address Book or ongoing conferences. ISDN/PSTN participants are added to the Address Book in the same manner that H.323 and SIP participants are added.(ISDN participants are not supported with Collaboration Server 1800).

When adding dial-out participants to the ongoing conference, the system automatically dials out to the participants using the Network Service (ISDN/PSTN or IP) defined for the connection in the participant properties.

Adding a New participant to the Address Book Directly

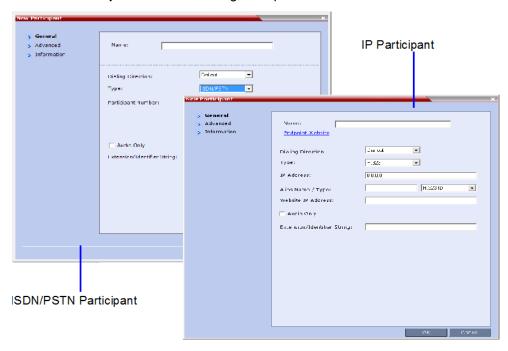
You can add a new participant to the **Main** group or to a group in the Address Book. Additionally, you can add a participant from a new conference, ongoing conference, or Conference Template.

ISDN participants are not supported with Collaboration Server 1800.

To add a new participant to the Address Book:

- 1 In the Address Book Navigation pane, select the group to where you want to add the new participant.
- 2 Click the **New Participant** button () or right-click the group to where you want to add the participant and select the **New Participant** option.
 - > Alternatively, click anywhere in the **List** pane and select the **New Participant** option.

The **New Participant - General** dialog box opens.



3 Define the following fields:

New Participant - General

Field	Description
Name	Enter the name of the participant or the endpoint as it will be displayed in the
	Collaboration Server Web Client.
	The Name field can be modified using Unicode encoding.
	 English text uses ASCII encoding and can contain the most characters (length varies according to the field).
	 European and Latin text length is approximately half the length of the maximum.
	Asian text length is approximately one third of the length of the maximum.
	Maximum field length in ASCII is 80 characters.
	The maximum length of text fields varies according to the mixture of character sets used (Unicode and ASCII).
	This field may not be left blank. Duplicate participant names, comma, and semi-color characters may not be used in this field.
	This name can also become the endpoint name that is displayed in the video layout. For more details about endpoint (site) names, see the <i>Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide</i> , Audio and Visual Indications (AVC CP Conferencing).
	Note: This field is displayed in all tabs.
Endpoint Website	Click the Endpoint Website hyperlink to connect to the internal website of the
(IP only)	participant's endpoint. It enables you to perform administrative, configuration and troubleshooting activities on the endpoint.
	The connection is available only if the IP address of the endpoint's internal site is defined in the Website IP Address field.
	Note: Endpoint Website hyperlinks are not supported when the Collaboration Server 1500/2000/4000 is in Ultra Secure Mode . For more information see Ultra Secure Mode . Ultra Secure Mode is not supported with Collaboration Server 1800.
Dialing Direction	Select the dialing direction:
Ū	Dial-in – The participant dials in to the conference. This field applies to IP participants only.
	Dial-out – The MCU dials out to the participant.
	Note:
	 Dial-out is forced when defining an ISDN/PSTN participant.
Туре	The network communication protocol used by the endpoint to connect to the conference: H.323 , or SIP or ISDN/PSTN .
	The fields in the dialog box change according to the selected network type.
IP Address	Enter the IP address of the participant's endpoint.
(H.323 and SIP)	 For H.323 participant define either the endpoint IP address or alias.
•	For SIP participant define either the endpoint IP address or the SIP address.
	For Collaboration Servers registered to a gatekeeper, the Collaboration Server can be configured to dial and receive calls to and from H.323 endpoints using the IP address in the event that the Gatekeeper is not functioning.
	Note: This field is hidden when the ISDN/PSTN protocol is selected.

New Participant - General (Continued)

Field	Description
Phone Number (ISDN/PSTN Only)	Enter the phone number of the ISDN/PSTN participant. Note: This field is only displayed when the ISDN/PSTN protocol is selected. ISDN participants are not supported with Collaboration Server 1800.
Alias Name/Type (H.323 Only)	If you are using the endpoint's alias and not the IP address, first select the type of alias and then enter the endpoint's alias: H.323 ID (alphanumeric ID) E.164 (digits 0-9, * and #) Email ID (email address format, e.g. abc@example.com) Participant Number (digits 0-9, * and #) Notes: Although all types are supported, the type of alias is dependent on the gatekeeper's capabilities. The most commonly supported alias types are H.323 ID and E.164. This field is used to enter the Entry Queue ID, target Conference ID and Conference Password when defining a cascaded link. Use of the E.164 Number is dependent on the setting of the REMOVE_IP_IF_NUMBER_EXISTS System Flag. For more information see Substituting E.164 Number in Dial String.
SIP Address/Type (SIP Only)	 Select the format in which the SIP address is written: SIP URI - Uses the format of an E-mail address, typically containing a user name and a host name: sip:[user]@[host]. For example, sip:dan@polycom.com. Note: If the SIP Address field contains an IPv6 address, it must be surrounded by square brackets, for example, [::1]. TEL URI - Used when the endpoint does not specify the domain that should interpret a telephone number that has been input by the user. Rather, each domain through which the request passes would be given that opportunity. For example, a user in an airport might log in and send requests through an outbound proxy in the airport. If the users enters 411 (this is the phone number for local directory assistance in the United States), this number needs to be interpreted and processed by the outbound proxy in the airport, and not by the user's home domain. In this case, tel: 411 is the correct choice. Note: This field is removed from the dialog box when the ISDN/PSTN protocol is selected.
Endpoint Website IP Address (IP only)	Enter the IP address of the endpoint's internal site to enable connection to it for management and configuration purposes. This field is automatically completed the first time that the endpoint connects to the Collaboration Server. If the field is blank it can be manually completed by the system administrator. The field can be modified while the endpoint is connected
Audio Only	Select this check box to define the participant as a voice participant, with no video capabilities.

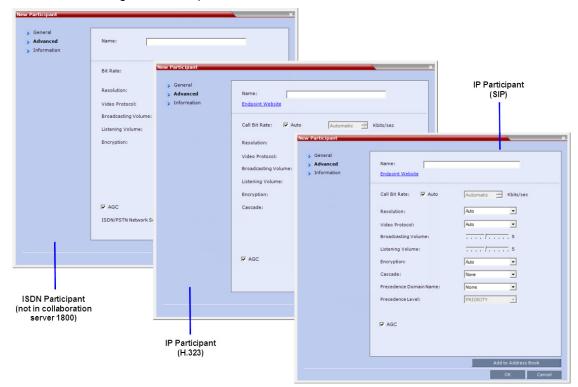
New Participant - General (Continued)

Field	Description
Extension/Identifier String	Dial-out participants that connect to an external device such as Cascaded Links or Recording Links may be required to enter a conference password or an identifying string to connect. Enter the required string as follows:
	[p][p][string]
	For example: pp4566#
	${f p}$ (optional) - Indicates a pause of one second before sending the DTMF string. Enter several concatenated [p]s to increase the delay before sending the string. The required delay depends on the configuration of the external device or conference IVR system.
	String - Enter the required string using the digits 0-9 and the characters * and #. The maximum number of characters that can be entered is identical to the H.323 alias length.
	If the information required to access the device/conference is composed of several strings, for example, the conference ID and the conference password, this information can be entered as one string, where pauses [p] are added between the strings for the required delays, as follows:
	[p][p][string][p][p] [string]
	For example: p23pp*34p4566#
Extension/Identifier String	The Collaboration Server automatically sends this information upon connection to the destination device/conference. The information is sent by the Collaboration Server as DTMF code to the destination device/conference, simulating the standard IVR procedure.

4 Usually, additional definitions are not required and you can use the system defaults for the remaining parameters. In such a case, click **OK**.

To modify the default settings for advanced parameters, click the **Advanced** tab.

5 Define the following **Advanced** parameters:



New Participant - Advanced

Field	Description
Video Bit Rate / Auto (IP Only)	The Auto check box is automatically selected to use the Line Rate defined for the conference.
	Note: This check box cannot be cleared when defining a new participant during an ongoing conference.
	To specify the video rate for the endpoint, clear this check box, and then select the required video rate.
Video Protocol	Select the video compression standard that will be forced by the MCU on the endpoint when connecting to the conference: H.261 , H.263 , H.264 or RTV . Select Auto to let the MCU select the video protocol according to the endpoint's capabilities.
Resolution	The Auto check box is automatically selected to use the Resolution defined for the conference.
	To specify the Resolution for the participant, select the required resolution from the drop-down menu.
Broadcasting Volume + Listening Volume	To adjust the volume the participant broadcasts to the conference or the volume the participant hears the conference, move the slider; each unit represents an increase or decrease of 3 dB (decibel). The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default connection value is 5.

New Participant - Advanced (Continued)

Field	Description
Encryption	Select whether the endpoint uses encryption for its connection to the conference. Auto (default setting) indicates that the endpoint will connect according to the conference encryption setting.
AGC	AGC (Auto Gain Control) mechanism regulates noise and audio volume by keeping the received audio signals of all participants balanced. Select this check box to enable the AGC mechanism for participants with weaker audio signals. Notes: • To be enable AGC, set the value of the ENABLE_AGC System Flag in system.cfg to YES. The flag's default value is NO. • If the System Flag does not exist in the system, it must be manually added to the System Configuration. For more information see Modifying System Flags. • Enabling AGC may result in amplification of background noise.
Cascaded (IP Only)	 If this participant is used as a link between conferences select: Slave, if the participant is defined in a conference running on a Slave MCU. Master, if the participant is defined in a conference running on the Master MCU. It enables the connection of one conference directly to another conference using an H.323 connection only. The conferences can run on the same MCU or different MCU's. For more information, see Basic Cascading using IP Cascaded Link.
Precedence Domain Name (Dial-out SIP Only)	When Multi Level Precedence and Preemption is used, this is the Precedence Domain Name for the participant. For more information see MLPP (Multi Level Precedence and Preemption).
Precedence Level (Dial-out SIP Only)	When Multi Level Precedence and Preemption is used, this is the Precedence Level for the participant For more information see MLPP (Multi Level Precedence and Preemption).
AGC	The Audio Gain Control (AGC) protocol that reduces noises is enabled by default for the participants. Clear this check box to disable the AGC feature.
ISDN/PSTN Network Service	Enables you to select the ISDN/PSTN network service. ISDN participants are not supported with Collaboration Server 1800.

6 To add general information about the participant, such as e-mail, company name, and so on, click the **Information** tab and type the necessary details in the **Info 1-4** fields. Text in the **info** fields can be added in Unicode format (length: 31 characters).

7 Click OK.

The new participant is added to the selected group in the address book.

Substituting E.164 Number in Dial String

Between the time a conference is scheduled and when it becomes active, the IP of an endpoint may change, especially in an environment that uses DHCP. The MCU can be set to ignore the IP address of a participant when the conference starts. Instead, the alternative E.164 number will be used.

The flag, **REMOVE_IP_IF_NUMBER_EXISTS** controls this option. This flag must be manually added to change its value. The values of this flag are:

- YES (default) The IP address of an endpoint will be ignored.
- NO The IP address of an endpoint will be used.

Guidelines for Substituting E.164 Number in Dial String

- When this feature is enabled, the IP address field of participants in scheduled conferences and conference templates will be empty.
- In order for the MCU to ignore the IP of H.323 participants, the following requirements must be met:
 - > A gatekeeper must be defined.
 - > The alias of the participant must be defined.
 - The alias type must be defined (not set to **None**).
- If an H.323 gatekeeper is defined but is not connected, the MCU will fail to connect to H.323 dial-out participants.
- In order for the MCU to ignore the IP of SIP participants, the following requirements must be met:
 - A SIP proxy must be defined.
 - > The SIP address must be defined.
- If a SIP proxy is defined but is not connected, the MCU will fail to connect to SIP dial-out participants.

Adding a Participant from an Ongoing Conference to the Address Book

You can add a participant to the Address Book directly from an ongoing conference.



When adding a participant to the address book from a new conference, **Participants** list of an ongoing conference or **Conference Template**, the participant is always added to the "Main" group.

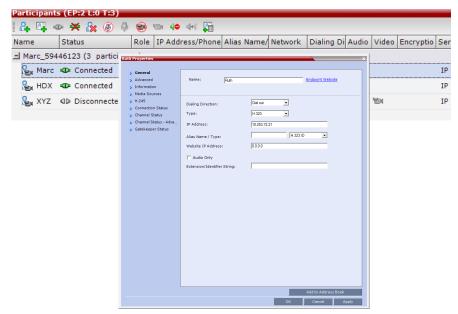
To add a participant from the conference to the Address Book:

1 During an ongoing conference, select the participant in the *Participant* pane, and either click the **Add Participant to Address Book** button (), or right-click and select **Add Participant to Address Book**.

The participant is added to the Address Book.

Alternatively, you could:

a Double-click the participant's icon, or right-click the participant icon and select **Participant Properties**.



The **Participant Properties** window opens.

b Click the **Add to Address Book** button.



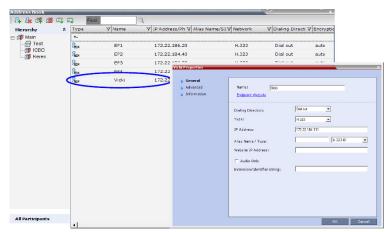
If the participant name is already listed in the All Participants list, an error message is displayed. In such a case, change the name of the participant before adding the participant to the address book.

Modifying Participants in the Address Book

When required, you can modify the participant's properties.

To modify participant properties in the Address Book:

- 1 In the Address Book Navigation pane, select the group to where the participant to modify is listed.
- 2 In the Address Book List pane, double-click the participant's icon.



The **Participant's Properties** window is displayed.

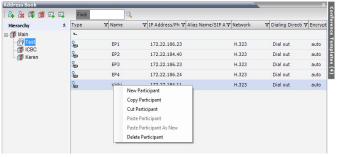
- 3 Modify the necessary properties in the window, such as dialing direction, communication protocol type, and so on. You can modify any property in any of the three tabs: **General, Advanced** and **Info**.
- 4 Click OK.

The changes to the participant's properties are updated.

Deleting Participants from the Address Book

To delete participants from the Address Book:

- 1 In the Address Book Navigation pane, select the group where the participant to delete is listed.
- 2 In the Address Book List pane, either select the participant to delete, and then select the Delete Participant (() button, or right-click the participant icon and then select the Delete Participant option.



- **3** A confirmation message is displayed depending on the participant's assignment to groups in the address book:
 - **a** When the participant belongs to only one group: click **Yes** to permanently delete the participant from the address book.
 - **b** When the participant belongs to multiple groups, a message is displayed requesting whether to delete the participant from the Address Book or from the current selected group. Select:
 - ♦ Current group to delete the participant from the selected group
 - ♦ Address Book to permanently delete the participant from the address book (all groups). Click **OK** to perform the delete operation, or **Cancel** to exit the delete operation.

Copying or Moving a Participant

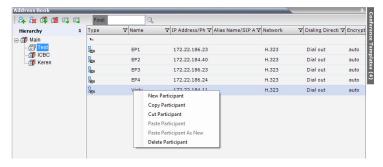
You can copy or move a participant from one group to another group using the **Copy**, **Cut**, and **Paste** options. A participant can belong to multiple groups. However, there is only one entity per participant. Groups that contain the same participants refer to the same definition of the participant entity. Alternatively, you can drag a participant from one location in the **Address Book** to another location, moving the participant to its new location using the drag-and-drop operation.



The cut and copy actions are not available when selecting multiple participants.

To copy or move a participant to another group:

- 1 In the Address Book Navigation pane, select the group from where to copy the participant.
- 2 In the Address Book List pane, select the participant you want to copy.
- **3** Right-click the selected participant, and select one of the following functions from the drop-down menu:



Copy / Move Participant

Function	Description
Copy Participant	Copies the participant to be pasted into an additional group.
Cut Participant	Moves the participant from the current group to a different group. Alternatively, you can move a participant to another location by dragging the participant to the new location.

- 4 In the **Address Book Navigation** pane, navigate and select the group in which you want to paste the participant.
- 5 Right-click the selected group, and click one of the following **Paste** functions from the drop-down menu:

Paste Participant

Function	Description
Paste Participant	Creates a link to the participant entity in the pasted location.

Paste Participant

Function	Description
Paste Participant as New	Pastes as a new participant into the selected group. This paste action adds "Copy" to the end of the participant name.



The Paste functions are only available after a **Copy** or **Cut** action has been implemented.

To drag a participant from an address book group to another group:

- 1 Select the participant or participants you want to move.
- **2** Click and hold the left mouse button and drag the selection to the new group. The participants are moved to the new address book group.

Searching the Address Book

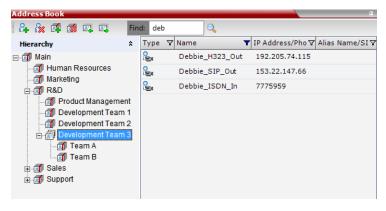
You can search the Address Book for a participant's name or a group name only on the currently selected group/level.

To search for participants or groups in the current selected level:

- 1 In the Address Book Navigation pane, select the group/level within to run the search.
- 2 In the Address Book toolbar, activate the search option by clicking the Find field.
 The field clears and a cursor appears indicating that the field is active.



3 Type all or part of the participant's name or group name and click the search button.



The closest matching participant entries are displayed and the Active Filter indicator turns on.

Filtering the Address Book

The entries in an address book group can be filtered to display only the entries (participants or groups) that meet criteria that you specify and hides entries that you do not want displayed. It enables you to select and work with a subset of **Address Book** entries.

You can filter by more than one column, by adding additional filters (columns).

The filter applies to the displayed group. If **All Participants** option is selected, it applies to all the listed participants.

Filtering can be done using:

- A predefined pattern
- Customized pattern

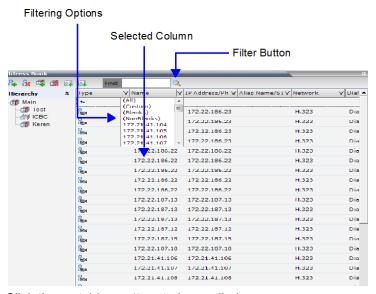
When you use the Find dialog box to search filtered data, only the data that is displayed is searched; data that is not displayed is not searched. To search all the data, clear all filters.

Filtering Address Book Data Using a Predefined Pattern

To filter the data in an address book group:

- 1 In the Address Book Navigation pane, select the group to filter.
- 2 In the Address Book List pane, in the column that you want to use for filtering, click the filter ()

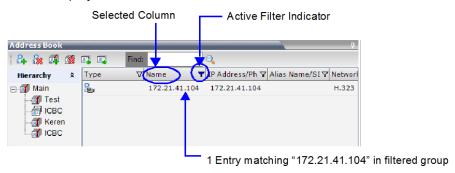
A drop-down menu is displayed containing all the matching patterns that can be applied to the selected field.



3 Click the matching pattern to be applied.

The filtered list is displayed with a filter indicator (\(\bar{Y}\)) displayed in the selected column heading.

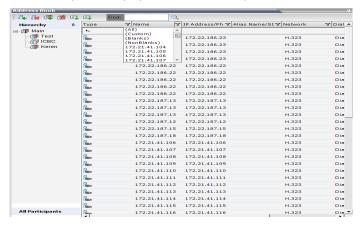
Example: If the user selects **172.21.41.104** as the matching pattern, the filtered group in the Address Book is displayed as follows:



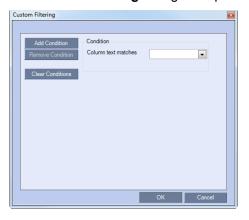
Filtering Address Book Data Using a Custom Pattern

To filter the data in an address book group:

- 1 In the Address Book Navigation pane, select the group to filter.
- 2 In the Address Book List pane, in the column that you want to use for filtering, click the filter (♥) button.
- 3 Select the (Custom) option from the drop-down list.



The **Custom Filtering** dialog box opens.

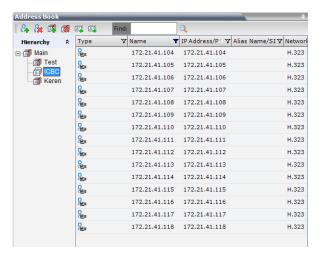


- 4 In the Condition Column text matches field, enter the filtering pattern.

 For example, to list only endpoints that include the numerals 41 in their name, enter 41.
- 5 To add filtering patterns to further filter the list or fine tune your search, click **Add Condition**.
- 6 To clear a filtering pattern, click Clear Condition.

The filtered list is displayed with an active filter (blue) indicator (\(\bar{\mathbb{T}}\)) displayed in the selected column heading.

For example, if the filtering pattern is 41, the participants list includes all the endpoints that contain the numerals 41 in their name.

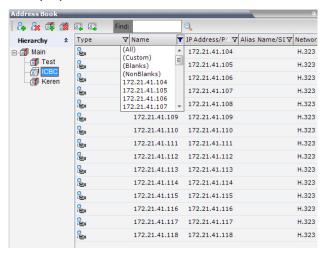


Clearing the Filter

To clear the filter and display all entries:

1 In the filtered Address Book column heading, click the Active Filter indicator. The pattern matching options menu is displayed.

2 Click (All).



The filter is deactivated and all the group/level entries are displayed.

Obtaining the Display Name from the Address Book

The MCU can be configured to replace the name of the dial-in participant as defined in the endpoint (site name) with the name defined in the Address Book.

In this process, the system retrieves the data (name, alias, number or IP address) of the dial-in participant and compares it first with the conference defined dial-in participants and if the endpoint is not found, it then searches for the endpoint with entries in the address book. After a match is found, the system displays the participant name as defined in the address book instead of the site name, in both the video layout and the Collaboration Server Web Client/Manager.

The system compares the following endpoint data with the address book entries:

- For H.323 participants, the system compares the IP address, Alias, or H.323 number.
- For SIP participants, the system compares the IP address or the SIP URI.

Guidelines for Obtaining the Display Name from the Address Book

- Only Users with Administrator and Operator Authorization Levels are allowed to enable and disable the Obtain Display Name from Address Book feature.
- This feature is supported for IPv4 participants only.

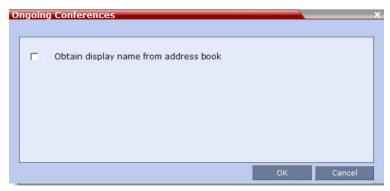
Enabling and Disabling the Obtain Display Name from Address Book Feature

The **Obtain Display Name from Address Book** option can be enabled for all participants connecting to the MCU if the name of the participants are defined in the Address Book.

To enable or disable the Obtain Display Name from Address Book option:

1 On the Collaboration Server main menu bar, select Setup > Customize Display Settings > Ongoing Conferences.

The **Ongoing Conferences** dialog box is displayed.



- 2 Select the Obtain display name from address book check box to enable the feature or clear the check box to disable the feature.
- 3 Click OK.

Importing and Exporting Address Books

Address Books are proprietary Polycom data files that can only be distributed among Collaboration Server units. The Address Books are exported in XML format, which are editable offline. If no name is assigned to the exported Address Book, the default file name is:

EMA.DataObjects.OfflineTemplates.AddressbookContent .xml

Exporting an Address Book

To Export an Address Book:

1 In the Address Book pane, click the **Export Address Book** (put) button, or right-click an empty area in the pane, and click **Export Address Book**.

The Export Address Book dialog box is displayed.



- 2 Enter the desired path, or click the **Browse** button.
- 3 In the **Save Address Book** dialog box, select the directory to save the file. You may also rename the file in the File Name field.
- 4 Click Save.

You will return to the **Export File** dialog box.

5 Click OK.

The exported Address Book is saved in the selected folder in XML format.

Importing an Address Book

To Import and Address Book:

1 In the Address Book pane, click the Import Address Book () button, or right-click an empty area in the pane, and then click Import Address Book.

The Import Address Book dialog box is displayed.



- 2 Enter the path from which to import the Address Book, or click the **Browse** button.
- 3 In the Open dialog box navigate to the desired Address Book file (in XML format) to import.



When importing an Address Book, participants with exact names in the current Address Book will be overwritten by participants defined in the imported Address Book.

4 Click Open.

You will return to the Import File dialog box.

5 Click OK.

The Address Book is imported and a confirmation message is displayed at the end of the process.

6 Click Close.

Upgrading and Downgrading Considerations (Collaboration Server 1500/2000/4000 only)

When upgrading to a multi-level address book version from a single-level address book, the following factors have to be taken into consideration:

- The system automatically creates a new address book with a different name and modifies the new address book to a multi-level hierarchical address book.
- By default, the address book contains two levels:
 - The top level (root) named Main.
 - Second level All address book groups from the single-level address book are placed under the Main group with their associated participants.
- Participants that were not previously associated with any group in the Address Book are placed in the Main group.
- All participants in the Address Book appear in the All Participants group.

• During the upgrade process, the single-level address book file is save in the system to enable a future the downgrade of the version to a previous, single-level address book version (if required).

When downgrading from a multi-level address book version to a single-level address book version, the multi-level address book is replaced during the downgrade process by the single-level address book that was saved during the upgrade process.

Integrating the Global Address Book (GAB) of Polycom RealPresence Resource Manager (XMA) or Polycom CMA™ with the Collaboration Server

The Polycom RealPresence Resource Manager (XMA) or Polycom CMA™ application includes a Global Address Book (GAB) with all registered endpoints. This address book can be used by the Collaboration Server users to add participants to conferences.

Guidelines for integrating with the Global Address Book of Polycom RealPresence Resource Manager (XMA) or Polycom CMA™

- The Collaboration Server can use only one address book at a time. After you integrate the Polycom RealPresence Resource Manager (XMA) or Polycom CMA with the Polycom Collaboration Server, the XMA/CMA address book replaces the Collaboration Server internal address book.
- The Collaboration Server uses the RealPresence Resource Manager (XMA) or Polycom CMA address book in read-only mode. You can only add or modify XMA/CMA address book entries from the RealPresence Resource Manager (XMA) or Polycom CMA.



The Collaboration Server acts as a proxy to all address book requests between the Collaboration Server Web Client and the XMA/CMA. **Ensure that firewall and other network settings allow the Collaboration Server access to the XMA or CMA server.**

To Integrate the RealPresence Resource Manager (XMA) or Polycom CMA Global Address Book (GAB) with the Collaboration Server:

- 1 In the RealPresence Resource Manager (XMA) or Polycom CMA application, manually add the Polycom Collaboration Server system to the RealPresence Resource Manager (XMA) or Polycom CMA system as directed in the RealPresence Resource Manager (XMA) or Polycom CMA Operations Guide.
- 2 In the RealPresence Resource Manager (XMA) or Polycom CMA application, add a user or use an existing user for Collaboration Server login as directed in the RealPresence Resource Manager (XMA) or Polycom CMA Operations Guide.

Write down the User Name and Password as they will be used later to define the Collaboration Server connection to the RealPresence Resource Manager (XMA) or Polycom CMA Global Address Book.

Collaboration Server Side

1 On the Collaboration Server menu, click Setup > System Configuration.

> MCMS_PARAMETERS_USER △ Value Flag Name >> CS_MODULE_PARAMETERS ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT NO BONDING_CHANNEL_DELAY ENABLE_AUTO_EXTENSION ENABLE_CASCADED_LINK_TO_JOIN_WITHO NO ENABLE_EXTERNAL_DB_ACCESS NO ENABLE_ISDN_REDIAL YES EXTERNAL_CONTENT_USER AUSTINCQS/Admin EXTERNAL_DB_DIRECTORY EXTERNAL_DB_IP EXTERNAL_DB_LOGIN POLYCOM EXTERNAL DB PASSWORD POLYCOM

The System Flags - MCMS_PARAMETERS_USER dialog box opens.

2 Modify the values of the flags in the table below.

For more information, see Modifying System Flags.

System Flags for CMA Address Book Integration

Flag	Description
EXTERNAL_CONTENT_ DIRECTORY	The Web Server folder name. Change this name if you have changed the default names used by the RealPresence Resource Manager (XMA) or Polycom CMA application. Default: /PlcmWebServices
EXTERNAL_CONTENT_ IP	Enter the IP address of the RealPresence Resource Manager (XMA) or Polycom CMA server. For example: 172.22.185.89.
	This flag is also the trigger for replacing the internal Collaboration Server address book with the RealPresence Resource Manager (XMA) or Polycom CMA Global Address Book (GAB).
	Leave this flag blank to disable address book integration with the RealPresence Resource Manager (XMA) or Polycom CMA server.
EXTERNAL_CONTENT_ PASSWORD	The password associated with the user name defined for the Collaboration Server in the RealPresence Resource Manager (XMA) or Polycom CMA server.
EXTERNAL_CONTENT_ USER	The login name defined for the Collaboration Server in the RealPresence Resource Manager (XMA) or Polycom CMA server defined in the format: domain name/user name.

- 3 Click **OK** to complete the definitions.
- **4** When prompted, click **Yes** to reset the MCU and implement the changes to the system configuration.

Scheduling Reservations

The Reservations option enables users to schedule conferences. These conferences can be launched immediately or become ongoing, at a specified time on a specified date.

Scheduling a conference reservation requires definition of conference parameters such as the date and time at which the conference is to start, the participants and the duration of the conference.

Scheduled conferences (Reservations) can occur once or repeatedly, and the recurrence pattern can vary.

The maximum number of reservations per Collaboration Server is:

- RealPresence Collaboration Server (RMX) 1500/1800/2000 2000
- RealPresence Collaboration Server (RMX) 4000 4000

Guidelines for Scheduling Reservations



Collaboration Server 1800 does not support

- · ISDN connections
- · Video Switching Conferencing Mode

System

By default, the Scheduler is enabled by a System Flag. The flag prevents potential scheduling
conflicts from occurring as a result of system calls from external scheduling applications such as
RealPresence Resource Manager, ReadiManager®, SE200, Polycom CMA™ and others via the API.

If an external scheduling application is used, the flag **INTERNAL_SCHEDULER** must be manually added to the System Configuration and its value must be set to **NO**.

For more information see Modifying System Flags.

Resources

- System resources are calculated according to the Collaboration Server's license. For more information, see Forcing Video Resource Allocation to CIF Resolution.
- System resource availability is partially checked when reservations are created:
 - If a conference duration extension request is received from an ongoing conference, the request is rejected if it would cause a resource conflict.
 - > If several reservations are scheduled to be activated at the same time and there are not enough resources for all participants to be connected:
 - ♦ The conferences are activated.
 - Participants are connected to all the ongoing conferences until all system resources are used up.

- If sufficient resources are not available in the system and a scheduled Reservation cannot be activated, the Reservation is deleted from the schedule.
- In RealPresence Collaboration Server (RMX) 1500/2000/4000, resources for Reservations are also calculated using the Reserve Resources for Audio/Video Participants fields of the New Reservation dialog box. For more information see Resources.
- Resources are reserved for participants at the highest video resolution supported by the Line Rate specified in the conference Profile and up to the maximum system video resolution specified by the Resolution Configuration dialog box.
- When a new Reservation is created in the Reservation Calendar, the effect of the new Reservation (including its recurrences) on available resources is checked. If resource deficiencies are found an error message is displayed.
 - Defined dial-in or dial-out participants, Meeting Rooms, Entry Queues and new connections to Ongoing conferences are not included in the resources calculation.

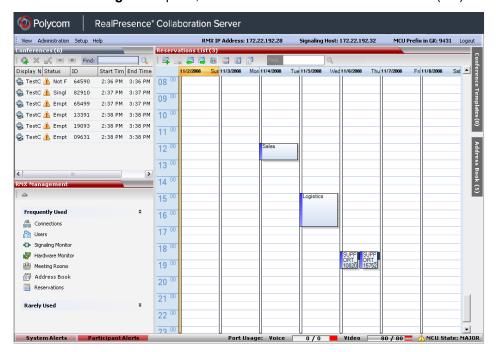
Reservations

- A Reservation that has been activated and becomes an ongoing conference is deleted from the Reservation Calendar list.
- The maximum number of concurrent reservations is 80. Reservations with durations that overlap (for any amount of time) are considered to be concurrent.
- System resource availability is partially checked when reservations are created:
 - > If a conference duration extension request is received from an ongoing conference, the request is rejected if it would cause a resource conflict.
 - If several reservations are scheduled to be activated at the same time and there are not enough resources for all participants to be connected:
 - The conferences are activated.
 - Participants are connected to all the ongoing conferences until all system resources are used up.
- A scheduled Reservation cannot be activated and is deleted from the schedule if:
 - An Ongoing conference has the same Numeric ID.
 - Sufficient resources are not available in the system.
- If a problem prevents a Reservation from being activated at its schedule time, the Reservation will
 not be activated at all. This applies even if the problem is resolved during the Reservation's
 scheduled time slot.
- A Profile that is assigned to a Reservation cannot be deleted.
- Reservations are backed up and restored during Setup > Software Management > Backup / Restore Configuration operations. For more information see Software Management.
- All existing reservations are erased by the Standard Restore option of the Administration > Tools
 > Restore Factory Defaults procedure.
- Reservations can also be scheduled from Conference Templates. For more information see Scheduling a Reservation From a Conference Template.

Using the Reservation Calendar

To open the Reservation Calendar:

• In the RMX Management pane, click the Reservation Calendar button ().



Toolbar Buttons

The toolbar buttons functions are described in the table below.

Reservations - Toolbar Buttons

Button	Description
New Reservation	Create a new reservation. The date and time of the new reservation is set according to the highlighted blocks on the Reservation Calendar .
Delete Reservation	Click to delete the selected reservation.
Back	Click to show the previous day or week, depending on whether Show Day or Show Week is the selected.
Next	Click to show the next day or week, depending on whether Show Day or Show Week is the selected.
Today	Click to show the current date in the Reservation Calendar in either Show Day or Show Week view.

Button	Description
Show Week	Change the calendar view to weekly display, showing a calendar week: Sunday through Saturday
Show Day	Click this button to show the day containing the selected time slot.
Reservations List	Click to change to List View and display a list of all reservations.
Find:	Used to search for reservations by Display Name. (Available in Reservations List view only).

Reservations Views

The Reservation Calendar list has the following views available:

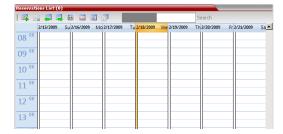
- Week
- Day
- Today
- List

In all views the Main Window List Pane header displays the total number of reservations in the system.



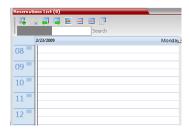
Week View

By default the Reservation Calendar is displayed in Week view with the current date highlighted in orange.



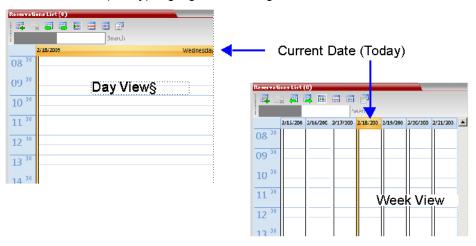
Day View

A single day is displayed.



Today View

The current date (Today), highlighted in orange, can be viewed in both Week View and Day View.

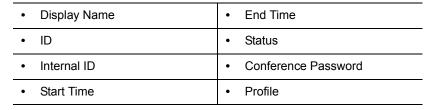


List View

List View does not have a calendar based format.



All Reservations are listed by:



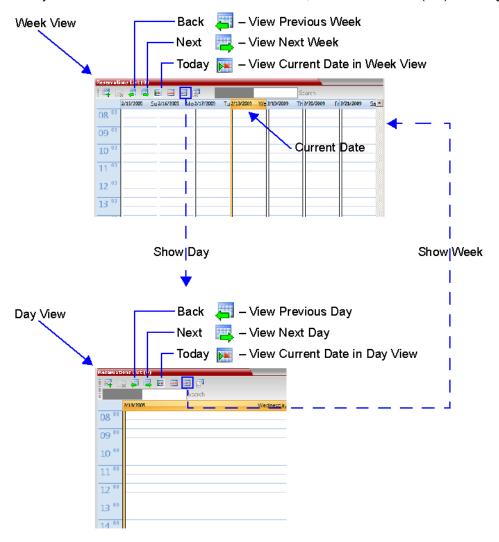
The Reservations can be sorted, searched and browsed by any of the listed fields.

Changing the Calendar View

To change between Week and Day views:

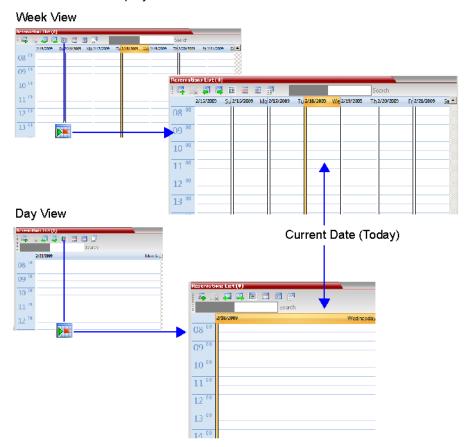
1 In Week View: In the **Reservation Calendar** toolbar, click **Show Day** () to change to Day View. or

In Day View: In the **Reservation Calendar** toolbar, click **Show Week** () to change to Week View.



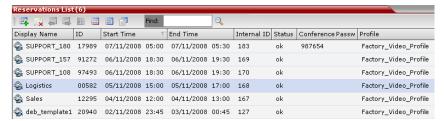
To view Today (the current date):

• In Week View or Day View, in the Reservation Calendar toolbar, click the **Today** () button to have the current date displayed within the selected view.



To change to List View:

1 In the Reservation Calendar toolbar, click, the **Reservations List** () button. The Reservations List is displayed.



2 To sort the data by any field (column heading), click on the column heading.

A ∇ or \triangle symbol is displayed in the column heading indicating that the list is sorted by this field, as well as the sort order.

3 To toggle the column's sort order, click on the column heading.

To return to Calendar View:

 In the Reservation Calendar toolbar, click any of the buttons (Show Week/Show Day/Today) to return to the required Reservation Calendar view.

Scheduling Conferences Using the Reservation Calendar

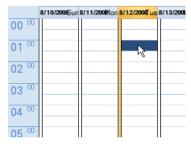
Creating a New Reservation

There are three methods of creating a new reservation:

- Method I Creating a reservation with default duration of 1 hour
- Method II Creating a reservation with default duration of ½ hour
- Method III Interactively define the reservation duration

Each method requires the selection of a starting time slot in the Reservation Calendar. The default time slot is the current half-hour period of local time.

In all views, if the **New Reservation** () button is clicked without selecting a starting time slot or if a time slot is selected that is in the past, the *Reservation* becomes an Ongoing conference immediately and is not added to the *Reservations* calendar.



After selecting a starting time slot in the Reservation Calendar you can create a reservation with a default duration derived from the creation method used or by interactively defining the duration of the reservation.

Method I - To create a reservation with default duration of 1 hour:

• In the Reservation Calendar toolbar, click the **New Reservation** () button to create a reservation of 1 hour duration.

Method II – To create a reservation with default duration of $\frac{1}{2}$ hour:

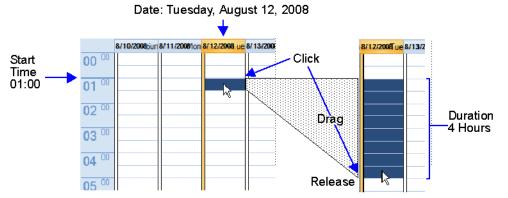
• Right-click and select **New Reservation** to create a reservation of ½ hour default duration.

Method III – To interactively define the duration:

1 In the calendar, click & drag to expand the time slot to select the required **Date**, **Start Time** and **Duration** for the reservation.

2 In the Reservation Calendar toolbar, click the New Reservation () button or right-click and select New Reservation.

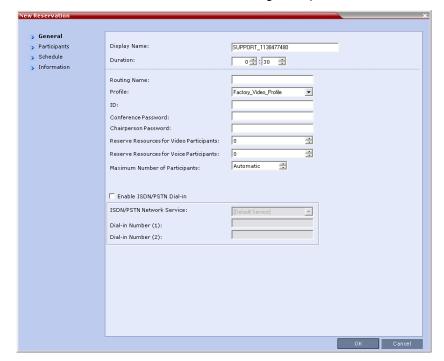
Example: The following click & drag sequence would select a reservation for Tuesday, August 12, 2008, starting at 01:00 with a duration of 4 hours.



The duration of reservations created by any of the above methods can be modified in the Scheduler tab of the New Reservation dialog box.

To create a new reservation:

- 1 Open the Reservation Calendar.
- **2** Select a starting time slot.
- **3** Create the reservation using one of the three methods described above.



The **New Reservation – General** tab dialog box opens.

All the fields are the same as for the **New Conference – General** dialog box, described in the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, General Tab.

New Reservation - Reserved Resources

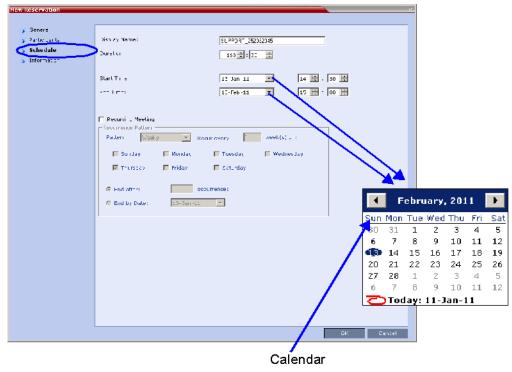
Field	Description
Reserve Resources for Video Participants	Enter the number of video participants for which the system must reserve resources. Default: 0 participants.
Reserve Resources for Audio Participants	Enter the number of audio participants for which the system must reserve resources. Default: 0 participants.



When a Conference Profile is assigned to a Meeting Room or a Reservation, the Profile's parameters are not embedded in the Reservation, and are taken from the Profile when the reservation becomes an ongoing conference. Therefore, any changes to the Profile parameters between the time the Reservation or Meeting Room was created and the time that it is activated (and becomes an ongoing conference) will be applied to the conference.

If the user wants to save the current parameters, a different Profile with these parameters must be assigned, or a different Profile with the new parameters must be created.

4 Click the Schedule tab.



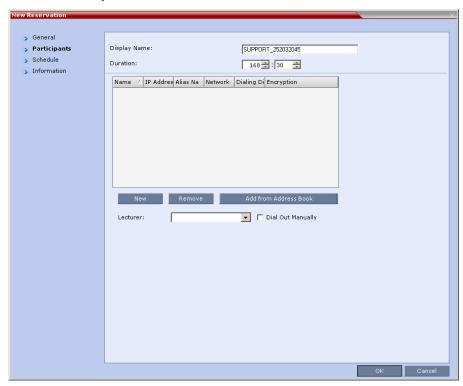
5 Adjust the new reservation's schedule by modifying the fields as described in the table below.

New Reservation - Schedule Tab

Field	Description		
Start Time	Select the Start Time of the Reservation.	•	ne Start/End Times of the Reservation are itially taken from the time slot selected in the eservation Calendar
End Time	Select the End Time of the Reservation.	th	ne Start/End Times can be adjusted by typing in e hours and minutes fields or by clicking the row buttons.
		th	ne Start/End dates can be adjusted by typing in e date field or by clicking the arrow buttons or sing the calendar.
		m int	ne start time of all the reservations can be anually adjusted in one operation. For more formation see Adjusting the Start Times of all eservations.
		Ti	nd Time settings are initially calculated as Start me + Duration. End Time settings are calculated if Start Time settings are changed.
		Ti	nanges to End Time settings do not affect Start me settings. However, the Duration of the eservation is recalculated.

Field	Description			
Recurring Meeting	Select this option to set up a Recurring Reservation - a series of Reservations to be repeated on a regular basis. To create a recurring reservation, you must define a time period and a recurrence pattern of how often the Reservation should occur: Daily , Weekly or Monthly .			
Recurrence Pattern	Daily	If Daily is selected, the system automatically selects all the days of the week. To de-select days (for example, weekends) clear their check boxes.		
	Weekly	If Weekly is selected, the system automatically selects the day of the week for the Reservation from the day selected in the Reservation Calendar. You can also define the recurrence interval in weeks. For example, if you want the reservation to occur every second week, enter 2 in the Recur every _ week(s) field. To define a twice-weekly recurring Reservation, select the check box of the additional day of the week on which the Reservation is to be scheduled and set the recurrence interval to 1. If Monthly is selected, the system automatically selects the day of the month as selected in the Reservation Calendar. You are required to choose a recurrence pattern:		
		 Day (1-31) of every (1-12) month(s) - Repeats a conference on a specified day of the month at a specified monthly interval. For example, if the first Reservation is scheduled for the 6th day of the current month and the monthly interval is set to 1, the monthly Reservation will occur on the 6th day of each of the following months. The (first, second,,last) (Sun-Sat) of x month(s) - Repeats a Reservation in a particular week, on a specified day of the week at the specified monthly interval. For example, a recurrent meeting on the third Monday every second month. 		
		can be set to end after a specified number of occurrences or by a of the following methods of terminating the series of Reservations:		
End After	End After: x Occurrences - Ends a recurring series of Reservations after a specific number (x) of occurrences. Default: 1 (Leaving the field blank defaults to 1 occurrence.)			
End by Date	End By Date: mm/dd/yyyy - Specifies a date for the last occurrence of the recurring series of Reservations. The End By Date value can be adjusted by typing in the date field or by clicking the arrow button and using the calendar utility. Default: Current date.			





The fields are the same as for the **New Conference – Participants** dialog box, described in the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Participants Tab.



Participant properties are embedded in the conferencing entity and therefore, if the participant properties are modified in the Address Book (or Meeting Rooms) after the Reservation has been created they are not applied to the participant when the Reservation is activated.

7 You can add participants from the Participants Address Book.

For more information see Meeting Rooms and the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, To add participants from the Address Book:.



Between the time a conference is scheduled and when it becomes active, the IP of an endpoint may change, especially in an environment that uses DHCP. The MCU can be set to ignore the IP address of a participant when the conference starts. Instead, the alternative E.164 number will be used instead of the IP address. For more information see Substituting E.164 Number in Dial String.

8 Optional. Add information to the reservation.

Information entered in the **Information** tab is written to the Call Detail Record (CDR) when the reservation is activated. Changes made to this information before it becomes an ongoing conference will be saved to the CDR.

For more information see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, Information Tab.

9 Click OK.

The New Reservation is created and is displayed in the **Reservation Calendar**.

If you create a recurring reservation all occurrences have the same ID. A recurring Reservation is assigned the same ISDN/PSTN dial-in number for all recurrences.

If a dial in number conflict occurs prior to the conference's start time, an alert is displayed: ISDN dial-in number is already assigned to another conferencing entity and the conference cannot start.

The series number (0000n) of each reservation is appended to its **Display Name**.

Example:

Conference Template name: Sales

Display Name for single scheduled occurrence:Sales

If 3 recurrences of the reservation are created:

Display Name for occurrence 1: Sales_00001

Display Name for occurrence 2: Sales_00002

Display Name for occurrence 3: Sales_00003

Managing Reservations

Reservations can be accessed and managed via all the views of the Reservations List.

Guidelines

- The Recurrence Pattern fields in the Schedule tab that are used to create multiple occurrences of a Reservation are only displayed when the Reservation and its multiple occurrences are initially created.
- As with single occurrence Reservations, only the **Duration**, **Start Time** and **End Time** parameters of
 multiple occurrence reservations can be modified after the Reservation has been created.
- A single occurrence Reservation cannot be modified to become a multiple occurrence reservation.
- Reservations can only be modified one at a time and not as a group.
- If Reservations were created as a recurring series, the system gives the option to delete them individually, or all as series.

Viewing and Modifying Reservations

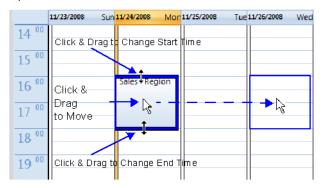
Reservations can be viewed and modified by using the **Week** and **Day** views of the **Reservations Calendar** or by using the **Reservation Properties** dialog box.

Using the Week and Day views of the Reservations Calendar

In the **Week** and **Day** views each Reservation is represented by a shaded square on the **Reservation Calendar**. Clicking on a Reservation selects the Reservation. A dark blue border is displayed around the edges of the Reservation indicating that it has been selected.

The **Start Time** of the Reservation is represented by the top edge of the square while the **End Time** is represented by the bottom edge.

The cursor changes to a vertical double arrow ($^{\updownarrow}$) when it is moved over the top and bottom sides of the square.



To move the Reservation to another time slot:

- 1 Select the Reservation.
- 2 Hold the mouse button down and drag the Reservation to the desired time slot.
- 3 Release the mouse button.

To change the Reservation's Start time:

- 1 Select the Reservation.
- 2 Move the mouse over the top edge of the Reservation's square.
- 3 When the cursor changes to a vertical double arrow ([↓]) hold the mouse button down and drag the edge to the desired **Start Time**.
- 4 Release the mouse button.

To change the Reservation's End time:

- 1 Select the Reservation.
- 2 Move the mouse over the bottom edge of the Reservation's square.
- 3 When the cursor changes to a vertical double arrow ([↓]) hold the mouse button down and drag the edge to the desired **End Time**.
- 4 Release the mouse button.

To View or Modify Reservations using the Reservation Properties dialog box:

- 1 In the Reservations List, navigate to the reservation (or its recurrences) you want to view, using the Show Day, Show Week, Today, Back, Next or List buttons.
- 2 Double-click, or right-click and select Reservation Properties, to select the reservation to be viewed or modified.
 - The Reservation Properties General dialog box opens.
- 3 Select the tab(s) of the properties you want to view or modify.
- 4 Optional. Modify the Reservation Properties.

5 Click OK.

The dialog box closes and modifications (if any) are saved.

Adjusting the Start Times of all Reservations

When utilizing GMT offset (for example, Daylight Saving Time change), the start time of the reoccurring reservations scheduled before the Collaboration Server time change are not updated accordingly (although their start times appear correctly in the Reservations list, when checking the reservation properties the start time is incorrect).

Following the Collaboration Server time change, the start time of all reoccurring reservations must be manually adjusted in one operation.

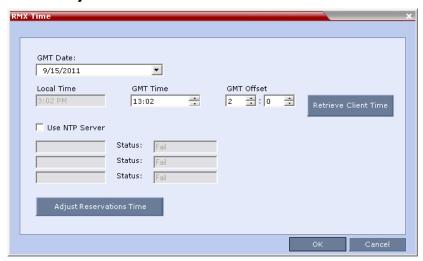
Using this option, the start times of **all** reservations currently scheduled on the Collaboration Server are adjusted with the same offset.

To adjust the reoccurring reservations start time after the GMT Offset has been changed for Daylight Saving Time (DST) or a physical move:

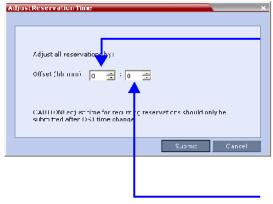


Adjustment of **Reservation Time** should only be performed after adjustment of Collaboration Server Time is completed as a separate procedure.

- 1 On the Collaboration Server menu, click Setup > RMX Time. The RMX Time dialog box opens.
- 2 Click the Adjust Reservations Time button.



The **Adjust Reservations Time** dialog box opens.



Click the arrows to adjust the start time by hours. Range is between 12 hours and -12 hours

A positive value indicates adding to the start time

Click the arrows to adjust the start time by minutes. Range is between 45 minutes and -45 minutes.

- 3 Click the arrows of the Offset Hours box to indicate the number of hours to add or subtract from the current start time; a positive value indicates adding time, while minus (-) indicates subtracting time.
- **4** Click the arrows of the **Offset minutes** box to indicate the number of minutes to add or subtract from the current start time of the reservations. Increments or decrements are by 15 minutes.
 - For example, to subtract 30 minutes from the start time of all the reservation, enter 0 in the **hours** box, and -30 in the **minutes** box.
 - To add one hour and 30 minutes to the start time, enter 1 in the hours box and 30 in the minutes box.
- 5 Click the **Adjust** button to apply the change to all the reoccurring reservations currently scheduled on the Collaboration Server.



When adjusting the start time of 1000 - 2000 reservations, an Internal communication error message may appear. Ignore this message as the process completes successfully.

Deleting Reservations

To delete a single reservation:

- 1 In the Reservations List, navigate to the reservation you want to delete, using the Show Day, Show Week, Today, Back, Next or List buttons.
- **2** Click to select the reservation to be deleted.
- 3 Click the **Delete Reservation** (★) button.

٥r

Place the mouse pointer within the Reservation block, right-click and select **Delete Reservation**.

4 Click **OK** in the confirmation dialog box.

The Reservation is deleted.

To delete all recurrences of a reservation:

- 1 In the Reservations List, navigate to the Reservation or any of its recurrences, using the **Show Day**, **Show Week**, **Today**, **Back**, **Next** or **List** buttons.
- 2 Click the **Delete Reservation** (\times) button.

or

Place the mouse pointer within the Reservation or any of its recurrences, right-click and select **Delete Reservation**.

A confirmation dialog box is displayed.



- 3 Select Delete the series.
- 4 Click OK.

All occurrences of the Reservation are deleted.

Searching for Reservations using Quick Search

Quick Search is available only in List View. It enables you to search for Reservations by **Display Name**.

To search for reservations:

1 In the Reservation Calendar toolbar, click in the Quick Search field.

The field clears and a cursor is displayed indicating that the field is active.



2 Type all or part of the reservation's **Display Name** into the field and click **Search**.

The closest matching Reservation entries are displayed.



3 To view or modify the Reservation:

 $\label{eq:continuous} \mbox{Double- click the Reservation's entry in the list to open the \textbf{Reservations Properties} \ \mbox{dialog box}.$

or

Right -click the Reservation's entry in the list and select a menu option to view, modify or delete the Reservation.

To clear the search and display all reservations:

- 1 Clear the Quick Search field.
- 2 Click Search.

All Reservations are displayed.

Operator Assistance & Participant Move



Operator conferences and participant move are supported in AVC CP Conferencing Mode only.

Users (operators) assistance to participants is available when:

- Participants have requested individual help (using *0 DTMF code) during the conference.
- Participants have requested help for the conference (using 00 DTMF code) during the conference.
- Participants have problems connecting to conferences, for example, when they enter the wrong conference ID or password.

In addition, the user (operator) can join the ongoing conference and assist all conference participants.

Operator assistance is available only when an Operator conference is running on the MCU.

The Operator conference offers additional conference management capabilities to the Collaboration Server users, enabling them to attend to participants with special requirements and acquire participant details for billing and statistics. This service is designed usually for large conferences that require the personal touch.

Operator Conferences

An Operator conference is a special conference that enables the Collaboration Server user acting as an operator to assist participants without disturbing the ongoing conferences and without being heard by other conference participants. The operator can move a participant from the Entry Queue or ongoing conference to a private, one-on-one conversation in the Operator conference.

In attended mode, the Collaboration Server user (operator) can perform one of the following actions:

- Participants connected to the Entry Queue who fail to enter the correct destination ID or conference password can be moved by the user to the Operator conference for assistance.
- After a short conversation, the operator can move the participant from the Operator conference to the appropriate destination conference (Home conference).
- The operator can connect participants belonging to the same destination conference to their conference simultaneously by selecting the appropriate participants and moving them to the Home conference (interactively or using the right-click menu).
- The operator can move one or several participants from an ongoing conference to the Operator conference for a private conversation.
- The operator can move participants between ongoing Continuous Presence conferences.

Operator Conference Guidelines

- An Operator conference can only run in Continuous Presence mode.
- Operator conference is defined in the Conference Profile. When enabled in Conference Profile, High Definition Video Switching option is disabled.
- An Operator conference can only be created by a User with Operator or Administrator Authorization level.
- Operator conference name is derived from the User Login Name and it cannot be modified.
- Only one Operator conference per User Login Name can be created.
- When created, the Operator conference must include one and only one participant the Operator participant.
- Only a defined dial-out participant can be added to an Operator conference as an Operator participant
- Once running, the Collaboration Server user can add new participants or move participants from other conferences to this conference. The maximum number of participants in an Operator conference is the same as in standard conferences.
- Special icons are used to indicate an Operator conference in the Ongoing Conferences list and the operator participant in the Participants list.
- An Operator conference cannot be defined as a Reservation.
- An Operator conference can be saved to a Conference Template. An ongoing Operator conference can be started from a Conference Template.
- The Operator participant cannot be deleted from the Operator conference or from any other conference to which she/he was moved to, but it can be disconnected from the conference.
- When deleting or terminating the Operator conference, the operator participant is automatically disconnected from the MCU, even if participating in a conference other than the Operator conference.
- Participants in Telepresence conferences cannot be moved from their conference, but an operator
 can join their conference and help them if assistance is required.
- Moving participants from/to an Operator conference follows the same guidelines as moving participants between conferences. For move guidelines, see <u>Move Guidelines</u>.
- When a participant is moved from the Entry Queue to the Operator conference, the option to move back to the source (Home) conference is disabled as the Entry Queue is not considered as a source conference.
- The conference chairperson cannot be moved to the Operator conference following the individual help request if the **Auto Terminate When Chairperson Exits** option is enabled, to prevent the conference from automatically ending prematurely. In such a case, the assistance request is treated by the system as a conference assistance request, and the operator can join the conference.

Defining the Components Enabling Operator Assistance

To enable operator assistance for conferences, the following conferencing entities must be adjusted or created:

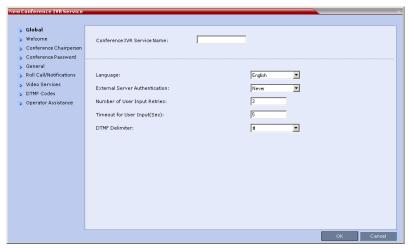
- IVR Service (Entry Queue and Conference) in which Operator Assistance options are enabled.
- A Conference Profile with the Operator Conference option enabled.
- An active Operator conference with a connected Operator participant.

Defining a Conference IVR Service with Operator Assistance Options

In the RMX Management pane, expand the Rarely Used list and click the IVR Services (iii) entry.

1 On the IVR Services toolbar, click the New Conference IVR Service () button.

The New Conference IVR Service - Global dialog box opens.



- 2 Enter the Conference IVR Service Name.
- 3 Define the Conference IVR Service Global parameters. For more information, see Conference IVR Service Properties Global Parameters.
- 4 Click the Welcome tab.
 - The New Conference IVR Service Welcome dialog box opens.
- 5 Define the system behavior when the participant enters the Conference IVR queue. For more information, see Defining a New Conference IVR Service.
- 6 Click the Conference Chairperson tab.
 - The New Conference IVR Service Conference Chairperson dialog box opens.
- 7 If required, enable the chairperson functionality and select the various voice messages and options for the chairperson connection. For more information, see New Conference IVR Service Properties -Conference Chairperson Options and Messages.
- 8 Click the Conference Password tab.
 - The New Conference IVR Service Conference Password dialog box opens.
- 9 If required, enable the request for conference password before moving the participant from the conference IVR queue to the conference and set the MCU behavior for password request for *Dial-in* and Dial-out participant connections. For more information, see New Conference IVR Service Properties - Conference Password Parameters.
- 10 Select the various audio messages that will be played in each case. For more information, see For more information, see New Conference IVR Service Properties Conference Password Parameters.
- 11 Click the General tab.
 - The **New Conference IVR Service General** dialog box opens.
- 12 Select the messages that will be played during the conference. For more information, see Conference IVR Service Properties - General Voice Messages.

13 Click the Roll Call/Notifications tab.

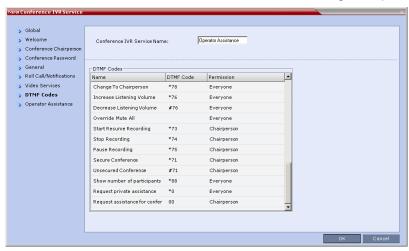
The New Conference IVR Service - Roll Call dialog box opens.

- 14 Enable the Roll Call feature and assign the appropriate audio file to each message type. For more information, see Conference IVR Service Properties - Roll Call Messages.
- 15 Click the Video Services tab.

The New Conference IVR Service - Video Services dialog box opens.

- 16 Define the Video Services parameters. For more information, see New Conference IVR Service Properties - Video Services Parameters.
- 17 Click the DTMF Codes tab.

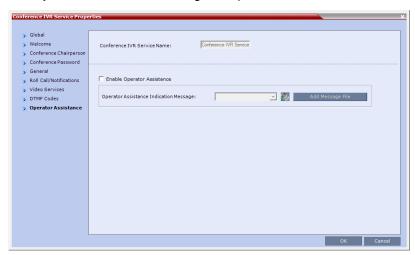
The New Conference IVR Service - DTMF Codes dialog box opens.



The default DTMF codes for the various functions that can be performed during the conference by all participants or by the chairperson are listed. For the full list of the available DTMF codes, see New Conference IVR Service Properties - DTMF Codes.

- **18** If required, modify the default DTMF codes and the permissions for various operations including Operator Assistance options:
 - ➤ *0 for individual help the participant requested help for himself or herself. In such a case, the participant requesting help is moved to the Operator conference for one-on-one conversation. By default, all participants can use this code.
 - > 00 for conference help the conference chairperson (default) can request help for the conference. In such a case, the operator joins the conference.
- 19 Click the Operator Assistance tab.

The Operator Assistance dialog box opens.



- **20** Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process to the conference or during the conference.
- **21** In the **Operator Assistance Indication Message** field, select the audio message to be played when the participant requests or is waiting for the operator's assistance.



If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the Collaboration Server.

22 Click **OK** to complete the IVR Service definition.

The new Conference IVR Service is added to the IVR Services list.

Defining an Entry Queue IVR Service with Operator Assistance Options

- 1 In the RMX Management pane, click IVR Services ().
- 2 In the IVR Services list, click New Entry Queue IVR Service ().
 The New Entry Queue IVR Service Global dialog box opens.
- 3 Define the Entry Queue Service Name.
- **4** Define the Entry Queue IVR Service Global parameters. For more information, see Entry Queue IVR Service Properties Global Parameters.
- 5 Click the Welcome tab.
 - The New Entry Queue IVR Service Welcome dialog box opens.
- 6 Define the system behavior when the participant enters the Entry Queue. This dialog box contains options that are identical to those in the Conference IVR Service Welcome Message dialog box.
- 7 Click the Conference ID tab.
 - The New Entry Queue IVR Service Conference ID dialog box opens.
- 8 Select the required voice messages. For more information, see Entry Queue IVR Service Properties Conference ID.

9 Click the Video Services tab.

The New Entry Queue IVR Service - Video Services dialog box opens.

- 10 In the Video Welcome Slide list, select the video slide that will be displayed to participants connecting to the Entry Queue. The slide list includes the video slides that were previously uploaded to the MCU memory.
- 11 Click the Operator Assistance tab.

The **Operator Assistance** dialog box opens.



- **12** Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process.
- **13** In the **Operator Assistance Indication Message** field, select the audio message to be played when the participant requests or is waiting for operator's assistance.



If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the Collaboration Server.

14 Click **OK** to complete the Entry Queue IVR Service definition.

The new Entry Queue IVR Service is added to the IVR Services list.

Defining a Conference Profile for an Operator Conference

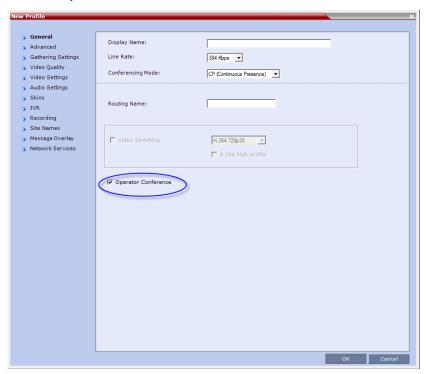
- 1 In the RMX Management pane, click Conference Profiles.
- 2 In the Conference Profiles pane, click New Profile.

The **New Profile – General** dialog box opens.

3 Define the Profile name and, if required, the Profile general parameters.

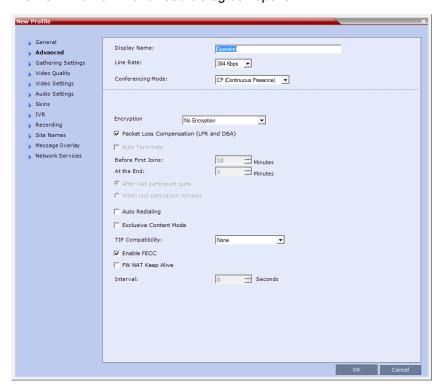
For more details, see New AVC CP Profile - General Parameters.

4 Click the Operator Conference check box.



5 Click the Advanced tab.

The New Profile - Advanced dialog box opens.



6 Define the **Profile - Advanced** parameters. For more details, see New AVC CP Profile - Advanced Parameters.

Note that when Operator Conference is selected, the **Auto Terminate** selection is automatically cleared and disabled and the Operator conference cannot automatically end unless it is terminated by the Collaboration Server User.

7 Click the Video Quality tab.

The New Profile - Video Quality dialog box opens.

- **8** Define the Video Quality parameters. For more details, see New AVC CP Profile Video Quality Parameters.
- 9 Click the Video Settings tab.

The **New Profile - Video Settings** dialog box opens.

- 10 Define the video display mode and layout. For more details, see New AVC CP Profile Video Settings Parameters.
- 11 Define the remaining Profile parameters. For more details, see Defining AVC CP Conferencing Profiles.
- **12** Click **OK** to complete the Profile definition.

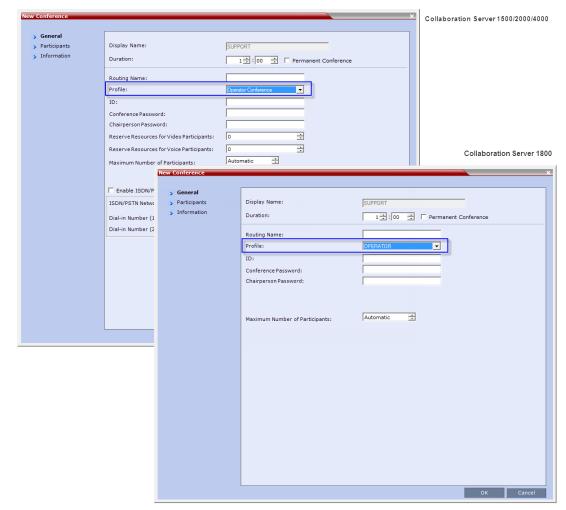
A new Profile is created and added to the Conference Profiles list.

Starting an Ongoing Operator Conference

To start a conference from the Conference pane:

1 In the Conferences pane, click New Conference (4).

The New Conference - General dialog box opens.



2 In the **Profile** field, select a Profile in which the **Operator Conference** option is selected.

Upon selection of the Operator Conference Profile, the **Display Name** is automatically taken from the Collaboration Server User Login Name. This name cannot be modified.

Only one Operator conference can be created for each User Login name.

3 Define the following parameters:

New Conference – General Options

Field	Description		
Duration	Define the duration of the conference in hours using the format HH:MM (default 01:00).		
	Notes:		
	 The Operator conference is automatically extended up to a maximum of 168 hours. Therefore, the default duration can be used. This field is displayed in all tabs. 		

Field	Description		
Routing Name	The name with which ongoing conferences, Meeting Rooms, Entry Queues and SIP Factories register with various devices on the network such as gatekeepers and SIP servers. This name must be defined using ASCII characters.		
	Comma, colon and semicolon characters cannot be used in the Routing Name .		
	The Routing Name can be defined by the user or automatically generated by the system if no Routing Name is entered as follows:		
	 If ASCII characters are entered as the Display Name, it is used also as the Routing Name 		
	 If a combination of Unicode and ASCII characters (or full Unicode text) is entered as the Display Name, the ID (such as Conference ID) is used as the Routing Name. 		
	If the same name is already used by another conference, Meeting Room or Entry Queue, the Collaboration Server displays an error message and requests that you to enter a different name.		
ID	Enter the unique-per-MCU conference ID. If left blank, the MCU automatically assigns a number once the conference is launched.		
	This ID must be communicated to conference participants to enable them to dial in to the conference.		
Conference Password	Leave this field empty when defining an Operator conference.		
Chairperson Password	Leave this field empty when defining an Operator conference.		
Reserve Resources for Video Participants	Enter the number of video participants for which the system must reserve resources.		
	Default: 0 participants.		
	When defining an Operator conference it is recommended to reserve resources for at least 2 video participants (for the operator and one additional participant - who will be moved to the Operator conference for assistance). Note: This option is not supported with Collaboration Server 1800.		
Reserve Resources for Audio Participants	Enter the number of audio participants for which the system must reserve resources.		
	Default: 0 participants.		
	When defining an Operator conference and the operator is expected to help voice participants, it is recommended to reserve resources for at least 2 video participants (for the operator and one additional participant - who will be moved to the Operator conference for assistance).		
	Note: This option is not supported with Collaboration Server 1800.		
Maximum Number of Participants	Enter the maximum number of participants that can connect to an Operator conference (you can have more than two), or leave the default selection (Automatic).		
	Maximum number of participants that can connect to an Operator conference:		

Field	Description		
Enable ISDN/PSTN Dial-in	Select this check box if you want ISDN and PSTN participants to be able to connect directly to the Operator conference. This may be useful if participants are having problems connecting to their conference and you want to identify the problem or help them connect to their destination conference. Note: ISDN connections are not supported with Collaboration Server 1800.		
ISDN/PSTN Network Service and Dial-in Number	If you have enable the option for ISDN/PSTN direct dial-in to the Operator conference, assign the ISDN/PSTN Network Service and a dial-in number to be used by the participants, or leave these fields blank to let the system select the default Network Service and assign the dial-in Number. Note: The dial-in number must be unique and it cannot be used by any other conferencing entity.		

4 Click the Participants tab.

The New Conference - Participants dialog box opens.

You must define or add the Operator participant to the Operator conference.

This participant must be defined as a **dial-out** participant.

Define the parameters of the endpoint that will be used by the Collaboration Server User to connect to the Operator conference and to other conference to assist participants.

For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Participants Tab.

- **5** To insert general information, select the **Information** tab.
 - The **Information** dialog box opens.
- **6** Enter the required information. For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Information Tab.
- 7 Click OK.

The new Operator conference is added to the ongoing Conferences list with a special icon The Operator participant is displayed in the Participants list with an Operator participant icon and the system automatically dials out to the Operator participant.

Saving an Operator Conference to a Template

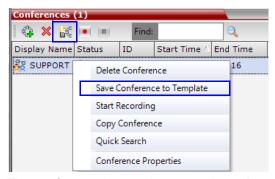
The Operator conference that is ongoing can be saved as a template.

To save an ongoing Operator conference as a template:

- 1 In the Conferences List, select the Operator conference you want to save as a Template.
- 2 Click the Save Conference to Template (button.

or

Right-click and select Save Conference to Template.



The conference is saved to a template whose name is taken from the ongoing conference **Display Name** (the Login name of the Collaboration Server User). The Template is displayed with the Operator Conference icon.



Starting an Operator Conference from a Template

An ongoing Operator conference can be started from an Operator Template saved in the Conference Templates list.

To start an ongoing Operator conference from an Operator Template:

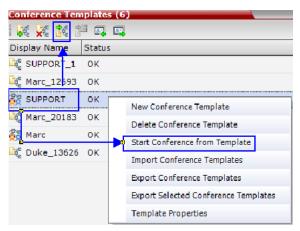
1 In the Conference Templates list, select the Operator Template to start as an ongoing Operator conference.



- You can only start an Operator conference from a template whose name is identical to your Login Name. For example, if your Login name is Polycom, you can only start an Operator conference from a template whose name is Polycom.
- If an ongoing Operator conference with the same name or any other conference with the same ID is already running, you cannot start another Operator conference with the same login name.
- 2 Click Start Conference from Template (...).

or

Right-click and select Start Conference from Template.



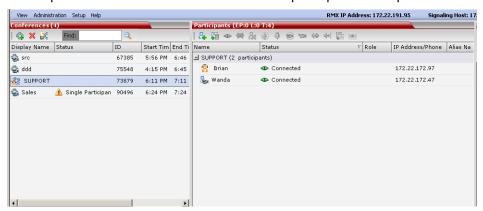
The conference is started.

The name of the ongoing conference in the *Conferences* list is taken from the Conference Template **Display Name**.

Monitoring Operator Conferences and Participants Requiring Assistance

Operator conferences are monitored in the same way as standard ongoing conferences.

Each Operator conference includes at least one participant - the Operator.



You can view the properties of the **Operator conference** by double-clicking the conference entry in the Conferences list or by right-clicking the conference entry and selecting **Conference Properties**. For more information, see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, Participant Level Monitoring.

Requesting Help

A participant can request help using the appropriate DTMF code from his/her touch tone telephone or the endpoint's DTMF input device. The participant can request *Individual Assistance* (default DTMF code *0) or Conference Assistance (default DTMF code 00).

Participants in Entry Queues who failed to enter the correct destination conference ID or the conference password will wait for operator assistance (provided that an Operator conference is active).

When requiring or requesting operator assistance, the Collaboration Server management application displays the following:



- The participant's connection Status changes, reflecting the help request. For more information, see table "Participants List Status Column Icons and Indications".
- The conference status changes and it is displayed with the exclamation point icon and the status Awaiting Operator.
- The appropriate voice message is played to the relevant participants indicating that assistance will be provided shortly.

The following icons and statuses are displayed in the **Participant Status** column:

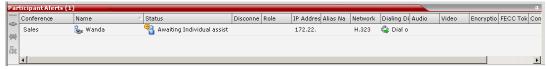
Participants List Status Column Icons and Indications

Icon	Status Indication	Description
	Awaiting Individual Assistance	The participant has requested the operator's assistance for himself/herself.
₽	Awaiting Conference Assistance	The participant has requested the operator's assistance for the conference. Usually this means that the operator is requested to join the conference.

When the Operator moves the participant to the Operator conference for individual assistance the participant Status indications are cleared.

Participant Alerts List

The **Participant Alerts** list contains all the participants who are currently waiting for operator assistance.



Participants are automatically added to the Participants Alerts list in the following circumstances:

- The participant fails to connect to the conference by entering the wrong conference ID or conference password and waits for the operator's assistance
- The participant requests Operator's Assistance during the ongoing conference

This list is used as reference only. Participants can be assisted and moved to the Operator conference or the destination conference only from the **Participants** list of the Entry Queues or ongoing conference where they are awaiting assistance.

The participants are automatically removed from the **Participant Alerts** list when moved to any conference (including the Operator conference).

Audible Alarms

In addition to the visual cues used to detect events occurring on the Collaboration Server, an audible alarm can be activated and played when participants request Operator Assistance.

Using Audible Alarms

The Audible Alarm functionality for Operator Assistance requests is enabled for each MCU in either the Collaboration Server Web Client or RMX Manager.

The Audible Alarm played when Operator Assistance is requested is enabled and selected in the **Setup > Audible Alarm > User Customization**. When the Audible Alarm is activated, the *.wav file selected in the *User Customization* is played, and it is repeated according to the number of repetitions defined in the *User Customization*.

If more than one Collaboration Server is monitored in the RMX Manager, the Audible Alarm must be enabled separately for each Collaboration Server installed in the site/configuration. A different *.wav file can be selected for each MCU.

When multiple Audible Alarms are activated in different conferences or by multiple MCUs, the Audible Alarms are synchronized and played one after the other. It is important to note that when **Stop Repeating Alarm** is selected from the toolbar from the Collaboration Server Web Client or RMX Manager, all activated Audible Alarms are immediately halted.

For more details on Audible alarms and their configuration, see Audible Alarms.

Moving Participants Between Conferences

The Collaboration Server User can move participants between ongoing conferences, including the Operator conference, and from the Entry Queue to the destination conference if help is required.

When moving between conferences or when a participant is moved from an Entry Queue to a conference by the Collaboration Server user (after failure to enter the correct destination ID or conference password), the IVR messages and slide display are skipped.

Move Guidelines

- Move is available only between CP conferences. Move is unavailable from/to Video Switching conferences (Collaboration Server 1500/2000/4000 only).
- Move between conferences can be performed without an active Operator conference.
- When moving the conference chairperson from his/her conference to another conference, the source
 conference will automatically end if the Auto Terminate When Chairperson Exits option is enabled
 and that participant is the only conference chairperson.
- When moving the Operator to any conference (following assistance request), the IVR messages and slide display are skipped.
- Participants cannot be moved from a Telepresence conference.

- Participants cannot be moved from LPR-enabled conferences to non-LPR conferences. Move from non-LPR conferences to LPR-enabled conferences is available.
- Move between encrypted and non-encrypted conferences depends on the ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF flag setting, as described in the following table:

Participant Move Capabilities vs. ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF flag setting

Flag Setting	Source Conference/EQ Encrypted	Destination Conference Encrypted	Move Enabled?
NO	Yes	Yes	Yes
NO	Yes	No	Yes
NO	No	Yes	No
NO	No	No	Yes
YES	Yes	Yes	Yes
YES	Yes	No	Yes
YES	No	Yes	Yes
YES	No	No	Yes

- When moving dial-out participants who are disconnected to another conference, the system automatically dials out to connect them to the destination conference.
- Cascaded links cannot be moved between conferences.
- Participants cannot be moved to a conference if the move will cause the number of participants to exceed the maximum number of participants allowed for the destination conference.

Moving Participants Options

Collaboration Server users can assist participants by performing the following operations:

- Move a participant to an Operator conference (Attend a participant).
- Move a participant to the Home (destination) conference.
- Move participant from one ongoing conference to another

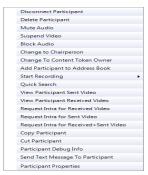
A move can be performed using the following methods:

- Using the participant right-click menu
- · Using drag and drop

To move a participant from the ongoing conference using the right-click menu options:

1 In the **Conferences** list, click the conference where there are participants waiting for Operator's Assistance to display the list of participants.

2 In the **Participants** list, right-click the icon of the participant to move and select one of the following options:



- > Move to Operator Conference to move the participant to the Operator conference.
- Move to Conference to move the participant to any ongoing conference.

When selected, the **Move to Conference** dialog box opens, letting you select the name of the destination conference.



➤ Back to Home Conference - if the participant was moved to another conference or to the Operator conference, this options moves the participant back to his/her source conference.

This option is not available if the participant was moved from the Entry Queue to the Operator conference or the destination conference.

Moving a Participant Interactively

You can drag and drop a participant from the Entry Queue or ongoing conference to the Operator or destination (Home) conference:

- 1 Display the participants list of the Entry Queue or the source conference by clicking its entry in the Conferences list.
- 2 In the Participants list, drag the icon of the participant to the **Conferences List** pane and drop it on the *Operator Conference* icon or another ongoing conference.

Conference Templates

Conference Templates enable administrators and operators to create, save, schedule and activate identical conferences.

A Conference Template:

- Saves the conference Profile.
- Saves all participant parameters including their Personal Layout and Video Forcing settings.
- Simplifies the setting up Telepresence conferences where precise participant layout and video forcing settings are crucial.

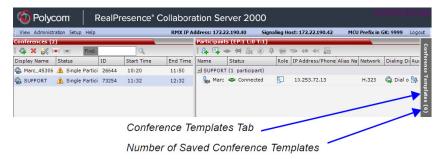
Guidelines

- The maximum number of templates is:
 - ➤ RealPresence Collaboration Server (RMX) 1500/1800/ 2000 100
 - ➤ RealPresence Collaboration Server (RMX) 4000 200
- A maximum of 200 participants can be saved in a Conference Template.
 - Trying to start a Conference Template that exceeds the allowed maximum number of participants will result in participants being disconnected due to resource deficiency.
- If the Profile assigned to a conference is deleted while the conference is ongoing the conference cannot be saved as a template.
- A Profile assigned to a Conference Template cannot be deleted. The system does not permit such a
 deletion.
- Profile parameters are not embedded in the Conference Template, and are taken from the Profile
 when the Conference Template becomes an ongoing conference. Therefore, any changes to the
 Profile parameters between the time the Conference Template was created and the time that it is
 activated (and becomes an ongoing conference) will be applied to the conference.
- Only defined participants can be saved to the Conference Template. Before saving a conference to a template ensure that all undefined participants have disconnected.
- Undefined participants are not saved in Conference Templates.
- Participant properties are embedded in the Conference Template and therefore, if the participant
 properties are modified in the Address Book after the Conference Template has been created they
 are not applied to the participant whether the Template becomes an ongoing conference or not.
- The Conference Template display name, routing name or ID can be the same as an Ongoing Conference, reservation, Meeting Room or Entry Queue as it is not active. However, an ongoing conference cannot be launched from the Conference Template if an ongoing conference, Meeting Room or Entry Queue already has the same name or ID. Therefore, it is recommended to modify the template ID, display name, routing name to be unique.
- A Reservation that has become an ongoing conference can be saved as Conference Template.

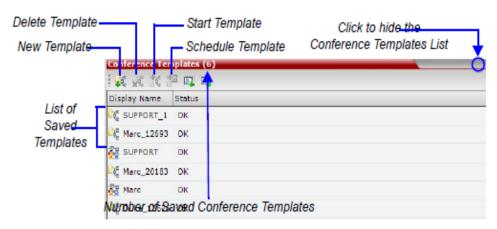
- SIP Factories and Entry Queues cannot be saved as Conference Templates.
- The conference specified in the Conference Template can be designated as a Permanent Conference. For more information see Permanent Conference.

Using Conference Templates

The Conference Templates list is initially displayed as a closed tab in the Collaboration Server Web Client main window. The number of saved **Conference Templates** is indicated on the tab.



Clicking the tab opens the Conference Templates list.



The Conference Templates are listed by Conference Template Display Name and ID and can be sorted by either field. The list can be customized by re-sizing the pane, adjusting the column widths or changing the order of the column headings.

For more information see *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide, Customizing the Main Screen*.

Clicking the anchor pin (button hides the Conference Templates list as a closed tab.

Toolbar Buttons

The Conference Template toolbar includes the following buttons:

Conference Templates - Toolbar Buttons

Button	Description
New Conference Template	Creates a new Conference Template.
Delete Conference Template	Deletes the Conference Template(s) that are selected in the list.
Start Conference from Template	Starts an ongoing conference from the Conference Template that has an identical name, ID parameters and participants as the template.
Schedule Reservation from Template	Creates a conference Reservation from the Conference Template with the same name, ID, parameters and participants as the Template. Opens the Scheduler dialog box enabling you to modify the fields
	required to create a single or recurring <i>Reservation</i> based on the template. For more information see Scheduling Reservations.

The Conferences List toolbar includes the following button:

Conferences List - Toolbar Button

Button	Description
Save Conference to Template	Saves the selected ongoing conference as a Conference Template.

Creating a New Conference Template



ISDN connections and Gateway calls are not supported with Collaboration Server 1800.

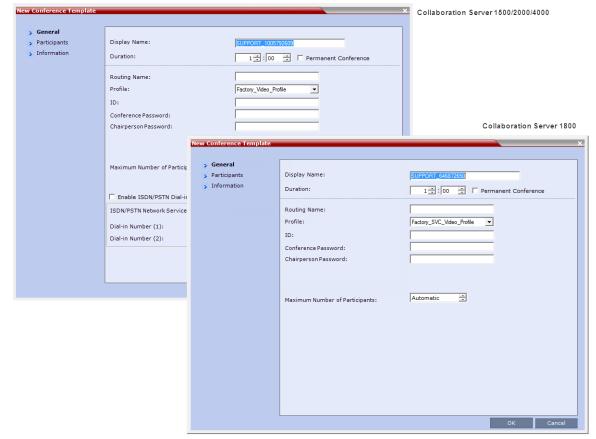
There are two methods to create a Conference Template:

- From scratch defining the conference parameters and participants
- Saving an ongoing conference as Template

Creating a new Conference Template from Scratch

To create a new Conference Template:

- 1 In the Collaboration Server main screen, click the **Conference Templates** tab.
- 2 Click the **New Conference Template** (button.



The **New Conference Template - General** dialog box opens.

The fields of the **New Template – General** dialog box are identical to those of the **New Conference – General** dialog box. For a full description of the fields see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, General Tab.

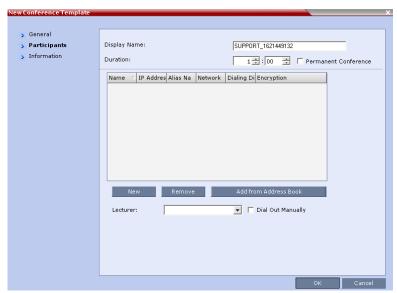
3 Modify the fields of the General dialog box.



A unique dial-in number must be assigned to each conferencing entity. However, Conference Templates can be assigned dial-in numbers that are already assigned to other conferencing entities, but when the template is used to start an ongoing conference or schedule a reservation, it will not start if another ongoing conference, Meeting Room, or Entry Queue or Gateway Profile is using this number.

4 Click the Participants tab.

The **New Template – Participants** dialog box opens.



The fields of the **New Template – Participants** dialog box are the same as those of the **New Conference – Participant** dialog box.

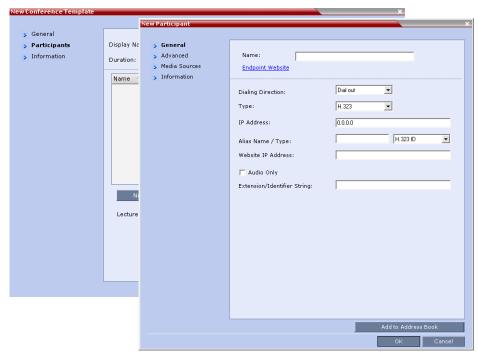
For a full description of these fields see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, Participants Tab.

5 You can add participants to the template from the Address Book as desired.

6 Click the New button.

The **New Participant – General** dialog box opens.

The New Template - Participant dialog box remains open in the background.

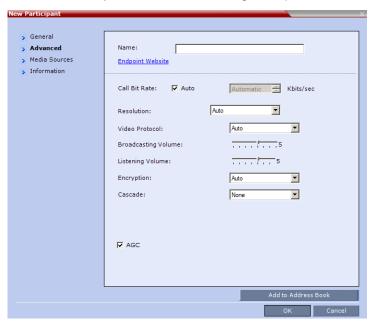


For a full description of the **General** tab fields see Adding a New participant to the Address Book Directly .

7 Modify the fields of the **General** dialog box.

8 Click the Advanced tab.

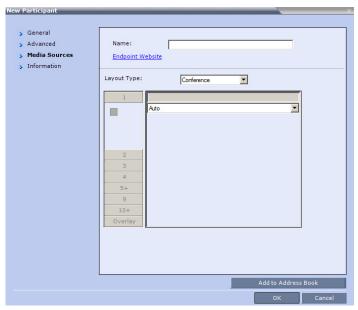
The **New Participant – Advanced** dialog box opens.



9 Modify the fields of the Advanced dialog box.

10 Click the Media Sources tab.

The **Media Sources** dialog box opens.



The **Media Sources** dialog box enables you to set up and save Personal Layout and Video Forcing settings for each participant. This is especially important when setting up Telepresence conferences.

For a full description of Personal Layout and Video Forcing settings see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Changing the Video Layout of a Conference (AVC-Based CP and Mixed CP and SVC Conferences) and Video Forcing (AVC-Based CP and Mixed CP and SVC Conferences).

- 11 Modify the Personal Layout and Video Forcing settings for the participant.
- **12** To add any optional information, click the **Information** tab.

The **New Participant – Information** dialog box opens.



For a full description of the Information fields see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide,* Information Tab .

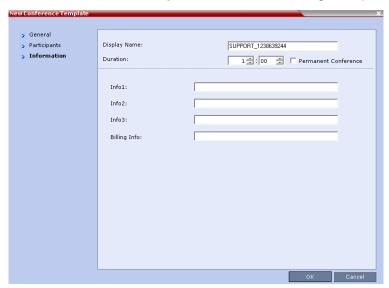
13 Click the OK button.

The participant you have defined is added to the Participants List.

The **New Participant** dialog box closes and you are returned to the **New Template – Participant** dialog box (which has remained open since step 6).

14 To add any optional information, in the **New Conference Template** dialog box, click the **Information** tab.

The **New Conference Template – Information** dialog box opens.



For a full description of the **Information** fields see the *Polycom RealPresence Collaboration Server* (RMX) 1500/1800/2000/4000 Getting Started Guide, Information Tab.

15 Click the OK button.

The New Conference Template is created and its name is added to the Conference Templates list.

Saving an Ongoing or AVC-based CP Operator Conference as a Template

Any ongoing or AVC-based CP Operator Conference can be saved as a template.

To save an ongoing or AVC-based CP Operator Conference as a template:

1 In the Conferences List, select the conference or Operator Conference to be saved as a Template.

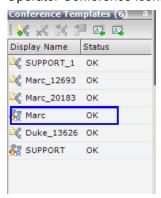
2 Click the Save Conference to Template (button.

or

Right-click and select **Save Conference to Template**.



The conference is saved to a template whose name is taken from the ongoing conference Display Name (the Login name of the Collaboration Server User). The Template is displayed with the Operator Conference icon.



Starting an Ongoing Conference From a Template



Conference Templates saved from an ongoing conference does not include Message Overlay text messages.

An ongoing conference can be started from any Template saved in the Conference Templates list. In SVC-based templates, only defined dial-in participants may be part of the conference.

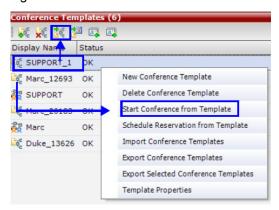
To start an ongoing conference from a Template:

1 In the Conference Templates list, select the Template you want to start as an ongoing conference.

2 Click the Start Conference from Template (button.

or

Right-click and select Start Conference from Template.



The conference is started.



In Collaboration Server 1500/2000/4000 Only.

If a Conference Template is assigned a dial-in number that is already assigned to an ongoing conference, Meeting Room, or Entry Queue or Gateway Profile, when the template is used to start an ongoing conference or schedule a reservation it will not start. However, the same number can be assigned to several conference templates provided they are not used to start an ongoing conference at the same time. If a dial in number conflict occurs prior to the conference's start time, an alert is displayed: ISDN dial-in number is already assigned to another conferencing entity and the conference cannot start.

The name of the ongoing conference in the Conferences list is taken from the Conference Template Display Name.

Participants that are connected to other ongoing conferences when the template becomes an ongoing conference are not connected.



If an ongoing conference, Meeting Room or Entry Queue with the same **Display Name**, **Routing Name** or **ID** already exists in the system, the conference will not be started.

Starting an Operator Conference from a Template (AVC Conferencing)

An ongoing Operator conference can be started from an Operator Template saved in the Conference Templates list.

To start an ongoing Operator conference from an Operator Template:

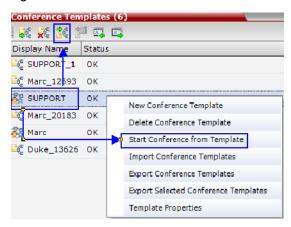
1 In the Conference Templates list, select the Operator Template to start as an ongoing Operator conference.



- You can only start an Operator conference from a template whose name is identical to your Login Name. For example, if your Login name is Polycom, you can only start an Operator conference from a template whose name is Polycom.
- If an ongoing Operator conference with the same name or any other conference with the same ID is already running, you cannot start another Operator conference with the same login name.
- 2 Click the Start Conference from Template (button.

or

Right-click and select **Start Conference from Template**.



The conference is started.

The name of the ongoing conference in the **Conferences** list is taken from the Conference Template **Display Name**.

Scheduling a Reservation From a Conference Template

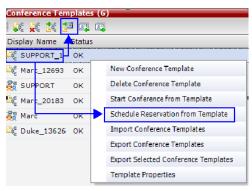
A Conference Template can be used to schedule a single or recurring Reservation.

To schedule a Reservation from a Conference Template:

- 1 In the Conference Templates list, select the Conference Template you want to schedule as a Reservation.
- 2 Click the Schedule Reservation from Template () button.

or

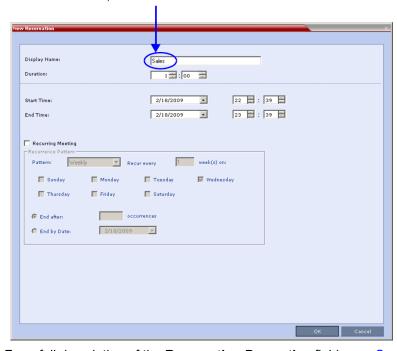
Right-click and select Schedule Reservation from Template.



The Reservation Properties dialog box is displayed.

The **Display Name** of the Reservation is taken from the Conference Template Display Name.

Conference Template and Reservation Name



For a full description of the Reservation Properties fields see Creating a New Reservation .

3 Modify the fields of the Reservation Properties.

4 Click the OK button.

A Reservation is created based on the Conference Template. The Reservation can be viewed and modified along with all other Reservations using the Reservations - Calendar View and Reservations List.

If you create a recurring reservation all occurrences have the same ID. A recurring Reservation is assigned the same ISDN/PSTN dial-in number for all recurrences.

If a dial-in number conflict occurs prior to the conference's start time, an alert is displayed: ISDN dial-in number is already assigned to another conferencing entity and the conference cannot start.

The series number (0000n) of each reservation is appended to its Display Name.

Example:

Conference Template name: Sales

Display Name for single scheduled occurrence:Sales

If 3 recurrences of the reservation are created:

Display Name for occurrence 1: Sales 00001

Display Name for occurrence 2: Sales_00002

Display Name for occurrence 3: Sales 00003

Deleting a Conference Template

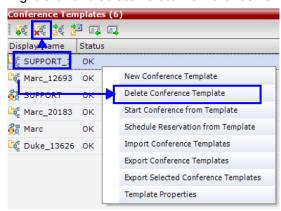
One or several Conference Templates can be deleted at a time.

To delete Conference Templates:

- 1 In the Conference Templates list, select the Template(s) you want to delete.
- 2 Click the **Delete Conference Template** (**) button.

or

Right-click and select **Delete Conference Template**.



A confirmation dialog box is displayed.

3 Click the **OK** button to delete the Conference Template(s).

Exporting and Importing Conference Templates

Conference Templates can be exported from one MCU and imported to multiple MCUs in your environment. Additionally, you can export Conference Templates and their associated Conference Profiles simultaneously. Using this option can save configuration time and ensures that identical settings are used for conferences running on different MCUs. This is especially important in environments using cascading conferences that are running on different MCUs.

- Administrators can export and import Conference Templates. Operators are only allowed to export Conference Templates.
- You can select a single, multiple or all Conference Templates to be exported.
- Both Conference Templates and their associated Conference Profiles can be exported and imported simultaneously when enabling the Export includes conference profiles or Import includes conference profiles options.
- Exporting and importing Conference Templates only can be used when you want to export and import individual Conference Templates without their associated Conference Profiles. This option enables you to import Conference Templates when Conference Profiles already exist on an MCU.

Exporting Conference Templates

Conference Templates are exported to a single XML file that can be used to import the Conference Templates on multiple MCUs.

Using the Export Conference Templates option, you can:

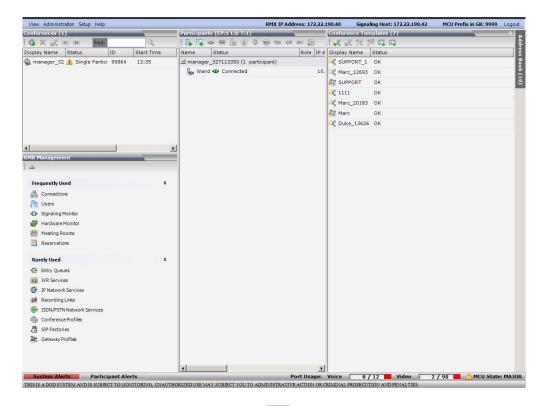
- Export all Conference Templates from an MCU
- Export selected Conference Templates

Exporting All Conference Templates from an MCU

To export all Conference Templates from an MCU:

1 In the Collaboration Server Web Client main window, click the Conference Templates tab.

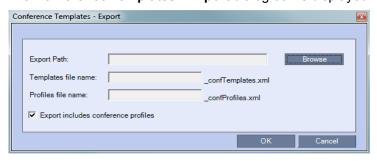
The **Conference Templates** list pane is displayed.



2 Click the Export Conference Templates button, or right-click the Conference Templates list, and then select Export Conference Templates.

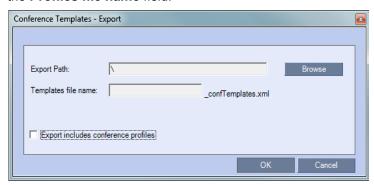


The Conference Templates - Export dialog box is displayed.



- 3 In the Export Path field, type the path name to the location where you want to save the exported file or click Browse to select the desired path.
- 4 If you wish to clear the **Export includes conference profiles** check box when you only want to export Conference Templates.

When this check box is cleared, the **Conference Templates - Export** dialog box is displayed without the **Profiles file name** field.



5 In the **Templates file name** field, type the file name prefix. The file name suffix (_confTemplates.xml) is predefined by the system. For example, if you type **Templates01**, the exported file name is defined as **Templates01_confTemplates.xml**.

The system automatically defines the Profiles file name field with the same file name prefix as the Templates file name field. For example, if you type Templates01 in the Templates file name field, the exported profiles file name is defined as **Templates01_confProfiles.xml**.

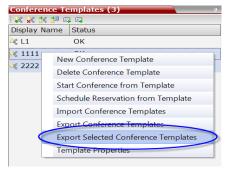
6 Click **OK** to export the Conference Templates and Conference Profiles to a file.

Exporting Selected Conference Templates

You can export a single Conference Template or multiple Conference Templates to other MCUs in your environment.

To export selected Conference Templates:

- 1 In the **Conference Templates** list, select the templates you want to export.
- 2 Right-click the Conference Templates to be exported, and then click **Export Selected Conference Templates**.



The Conference Templates - Export dialog box is displayed.



- 3 In the Export Path field, type the path name to the location where you want to save the exported file or click Browse to select the desired path.
- 4 To export Conference Templates, clear the **Export includes conference profiles** check box.

 When this check box is cleared, the **Conference Templates Export** dialog box is displayed without the Profiles file name field.



In the **Templates file name** field, type the file name prefix. The file name suffix (**_confTemplates.xml**) is predefined by the system. For example, if you type, Templates01, the exported file name is defined as **Templates01_confTemplates.xml**.

The system automatically defines the Profiles file name field with the same file name prefix as the Templates file name field. For example, if you type Templates01 in the Templates file name field, the exported profiles file name is defined as **Templates01_confProfiles.xml**.

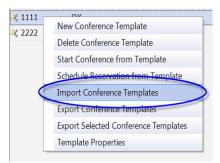
6 Click **OK** to export the Conference Templates and Conference Profiles to a file.

Importing Conference Templates

You can import Conference Templates and Conference Profiles from one MCU to multiple MCUs in your environment.

To import Conference Templates:

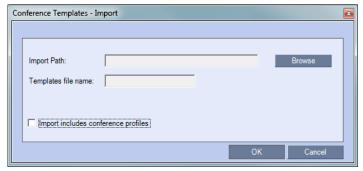
- 1 In the Collaboration Server Web Client main window, click the Conference Templates tab. The Conference Templates are displayed.
- 2 Click the **Import Conference Templates** button or right-click the Conference Templates pane, and then click **Import Conference Templates**.



The Conference Templates - Import dialog box is displayed.



3 To import Conference Templates, clear the Import includes conference profiles check box.
When this check box is cleared, the Conference Templates - Import dialog box is displayed without the Profiles file name field.



4 In the Import Path field, click Browse to navigate to the path and file name of the Conference Templates you want to import.

When clicking the exported templates file you want to import, the system automatically displays the appropriate files in the Templates file name field and the **Profiles file name** field (when the **Import includes conference profiles** check box is selected).

- **5** Click **OK** to import the Conference Templates and their associated Conference Profiles, if selected. Conference Templates are not imported when:
 - > A Conference Template already exists
 - > An associated Conference Profile is not defined in the Conference Profiles list

When one or more Conference Templates are not imported, a Message Alert window is displayed with the templates that were not imported.



6 Click Cancel to exit the Message Alerts window.

The imported Conference Templates are added to the Conference Templates list. When the **Import includes conference profiles** check box is selected, the imported Conference Profiles are added to the Conference Profiles list.

Polycom Conferencing for Microsoft Outlook®



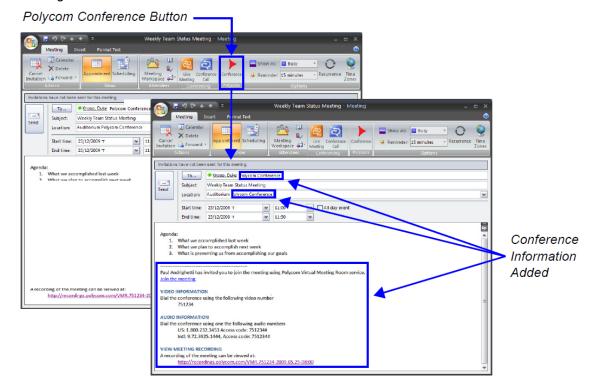
Polycom Conferencing for Microsoft Outlook is supported in AVC CP Conferencing Mode only

Polycom Conferencing for Microsoft Outlook is an add-in that enables users to easily organize and invite attendees to Video Enabled meetings via Microsoft Outlook®.

Polycom Conferencing for Microsoft Outlook is implemented by installing the Polycom Conferencing Add-in for Microsoft Outlook on Microsoft Outlook® e-mail clients. It enables meetings to be scheduled with video endpoints from within Outlook. The add-in also adds a Polycom Conference button in the **Meeting** tab of the Microsoft Outlook e-mail client ribbon.

The meeting organizer clicks the **Polycom Conference** button to add **Conference Information** to the meeting invitation.

Attendees call the meeting at the scheduled **Start Time** using the link or the dial-in number provided in the meeting invitation.



A Gathering Slide is displayed to connected participants until the conference starts.



The Gathering Slide displays live video along with information taken from the meeting invitation such as the subject, meeting organizer, duration, dial-in numbers etc. At the end of the Gathering Phase, the conference layout is displayed.

For more information see Video Preview (AVC Participants Only).

Setting up the Calendaring Solution

The following steps are performed to set up the Calendaring solution:

- **a** The administrator installs the Polycom Conferencing Add-in for Microsoft for Microsoft Outlook e-mail clients. For more information, see the Polycom Unified Communications Deployment Guide for Microsoft Environments.
- **b** The administrator creates an Microsoft Outlook e-mail-account for the Collaboration Server. If included in the solution, Polycom RealPresence DMA system and calendaring-enabled endpoints share this e-mail account. For more information, see the Polycom Unified Communications Deployment Guide for Microsoft Environments.
- c The administrator configures the Collaboration Server for Calendaring using the Exchange Integration Configuration dialog box, providing it with the Microsoft Exchange Server Name, User Name and Password and optional Primary SMTP Mail box information needed to access the e-mail account.

To configure the Collaboration Server's Exchange Integration Configuration:

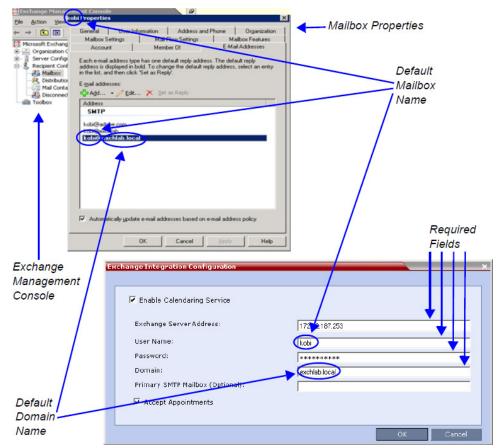
1 On the Collaboration Server menu, click **Setup > Exchange Integration Configuration**.

The **Exchange Integration Configuration** dialog box is displayed.



There are three options that can be used to configure the **Exchange Integration Configuration**. The option you choose will depend on the configuration of the mailbox in the Exchange Server and the configuration of the Exchange Server itself.

- > Option 1 Use this option if the Exchange Server settings have been left at their default values.
- > Option 2 Use this option if the Primary SMTP Mailbox is not the default mailbox.
- Option 3 Use this option if the Exchange Server settings have been modified by the administrator.



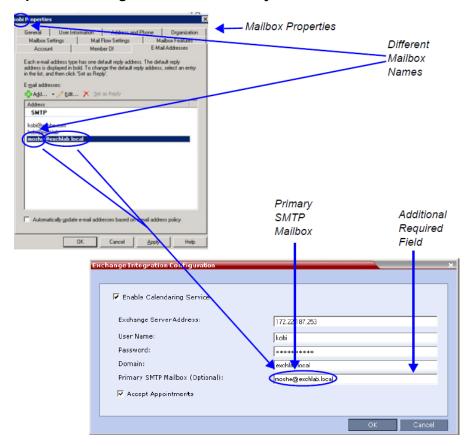
Option 1 - Using default Exchange Server settings

a Define the following fields:

Exchange Integration Configuration - Option 1

Field	Description
Enable Calendaring Service	Select or clear this check box to enable or disable the Calendaring Service using the Polycom Add-in for Microsoft Outlook. When this check box is cleared all fields in the dialog box are disabled.
Exchange Server Address	Enter the IP address of the Exchange Server.
User Name	Enter the User Name of the Collaboration Server, as registered in the Microsoft Exchange Server, that the Collaboration Server uses to login to its e-mail account. Field length: Up to 80 characters.
Password	Enter the Password the Collaboration Server uses to login to its e-mail account as registered in the Microsoft Exchange Server. Field length: Up to 80 characters.
Domain	Enter the name of the network domain where the Collaboration Server is installed as defined in the Microsoft Exchange Server.
Primary SMTP Mailbox (Optional)	This field is left empty.
Accept Appointments	Select this check box to enable the Collaboration Server to send replies to meeting invitations. Clear this check box when the Collaboration Server is part of a Unified Conferencing solution that includes a RealPresence DMA system, as the RealPresence DMA system will send a reply to the meeting invitation.

b Click **OK**.



Option 2 - Using an alternate Primary SMTP Mailbox

a Define the following fields:

Exchange Integration Configuration - Option 2

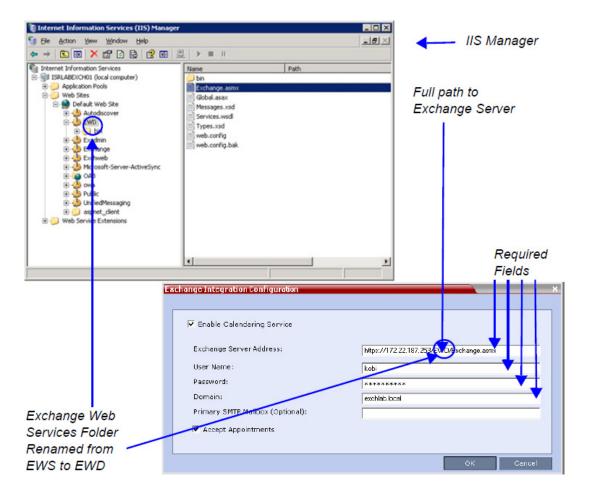
Field	Description
Enable Calendaring Service	These fields are defined as for Option 1 above.
Exchange Server Address	_
User Name	_
Password	_
Domain	-
Accept Appointments	_

Exchange Integration Configuration - Option 2 (Continued)

Field	Description
Primary SMTP Mailbox (Optional)	Enter the name of the SMTP Mailbox in the Microsoft Exchange Server to be monitored by the Collaboration Server.
	Note: Although several mailboxes can be assigned to each user in the Microsoft Exchange Server, only the Primary SMTP Mailbox is monitored. The Primary SMTP Mailbox name does not have to contain either the Collaboration Server's User Name or Domain name.

b Click OK.

Option 3 - Using modified Exchange Server settings



a Define the following fields:

Exchange Integration Configuration - Option 3

Field	Description
Exchange Server Address	If Exchange Server settings have been modified, enter the full path to the Microsoft Exchange Server where the Collaboration Server's Microsoft Outlook e-mail account is registered, for example if the EWS folder has been renamed EWD : https://labexch01/ EWD /Exchange.asmx
	Note: If a server name is entered, the Collaboration Server and the Microsoft Exchange Server must be registered to the same Domain. (The Domain name entered in this dialog box must match the Local Domain Name entry in the Management Network - DNS Properties dialog box.) For more information see Modifying the Default IP Network Service in the RealPresence Collaboration Server 800s. Field length: Up to 80 characters.
Enable Calendaring Service	These fields are defined as for Option 1 above.
User Name	
Password	
Domain	
Primary SMTP Mailbox (Optional)	
Accept Appointments	

b Click the **OK** button.

If applicable, RSS, VMC, RealPresence DMA system, and calendaring-enabled endpoints are configured with the **Exchange Server Name**, **User Names** and **Passwords** needed to access their accounts.

For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

1 The administrator configures the Collaboration Server to have a default Ad-hoc Entry Queue service enabled. If ISDN/PSTN participants are included, up to two ISDN/PSTN dial-in numbers must be configured for the Ad Hoc Entry Queue.

For more information see Defining a New Entry Queue.

Calendaring Guidelines

- The Collaboration Server must have its *MCU* prefix registered in the gatekeeper.
 - For more information see Modifying the Default IP Network Service.
- The Collaboration Server must be configured as a Static Route.
 - For more information see Modifying the Default IP Network Service.

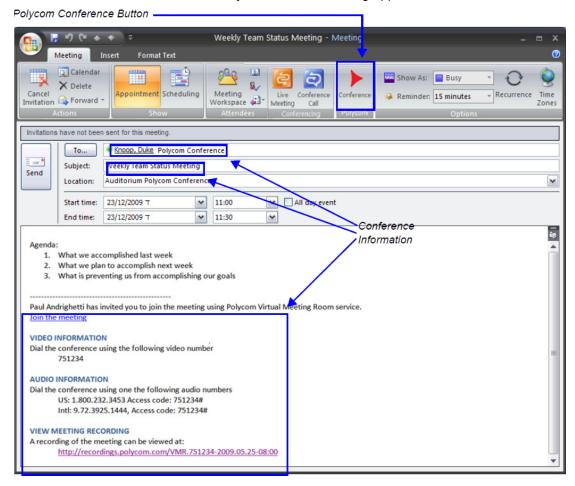
- The Collaboration Server's Default Entry Queue must be configured as an Ad Hoc Entry Queue and must be designated as the Transit Entry Queue.
 - For more information see the Entry Queues.
- The meeting organizer can enable recording and/or streaming of the meeting.
- If meeting is to be recorded, the Ad Hoc Entry Queue must have recording enabled in its Profile. For more information see Defining AVC CP Conferencing Profiles.
- Meetings can be single instance or have multiple occurrences.
- Attendees that do not have video devices may be invited to the meeting.
- Attendees using e-mail applications that use the iCalendar format may be invited to meetings via the Calendaring Service.
- Meeting invitations sent by Polycom Conferencing for Microsoft Outlook can be in a different language to the Collaboration Server Web Client. The following languages are supported:
 - > English
 - French
 - German
 - International Spanish
 - Korean
 - Japanese
 - > Simplified Chinese
- Collaboration Server resource management is the responsibility of the system administrator:
 - Conferences initiated by Polycom Conferencing for Microsoft Outlook are ad hoc and therefore resources are not reserved in advance.
 - Polycom Conferencing for Microsoft Outlook Add-in assumes that sufficient resources are available and does not check resource availability. Sufficient resources are therefore not guaranteed.
 - > A meeting invitation that is automatically accepted by the Collaboration Server is not guaranteed availability of resources.
 - If the Collaboration Server runs out of resources, attendees will not be able to connect to their conferences.
- By using RealPresence DMA system to load-balance resources between several Collaboration Servers, resource capacity can be increased, alleviating resource availability problems.

Creating and Connecting to a Conference

Creating a Conference

Meetings are organized using the Microsoft Outlook client in the normal manner.

If the meeting organizer decides that video participants are to be included in a multipoint video conference, he/she clicks the **Polycom Conference** button. Conference Information such as the **Meeting ID** and connection information is automatically added to the existing appointment information.



The meeting organizer can add a meeting agenda or personal text to the invitation before it is sent. The meeting organizer can update or cancel the video enabled meeting in the same manner as for any other meeting.

When the meeting organizer sends the meeting invitation a meeting record is saved in the Microsoft Exchange Server, the RealPresence Collaboration Server, RealPresence DMA system, RSS and calendaring-enabled endpoints.

RealPresence Collaboration Servers, RealPresence DMA system, and calendaring-enabled endpoints poll the Microsoft Exchange Server to retrieve new meeting records and updates to existing meeting records.

Microsoft Outlook Field Usage summarizes the Collaboration Server's usage of Microsoft Outlook data fields included in the meeting invitation.

Microsoft Outlook Field Usage

Microsoft	Usage by the Collaboration Server / R	on Server / RealPresence DMAsystem			
Outlook Field	Conference / Meeting Room	Gathering Slide			
Subject	Display Name of Conference / Meeting Room.	Meeting Name.			
Start/End Time	Used to calculate the Conference's Dura	tion.			
Record	Enable Recording in the Conference or Meeting Room Profile.	Display Recording option.			
Video Access Number	Comprised of: <mcu gatekeeper="" in="" prefix=""> <conference id="" numeric="">. Note: It is important that MCU Prefix in Gatekeeper field in the Collaboration Server's IP Network Service - Gatekeeper tab and the Dial-in prefix field in the Polycom Conferencing Add-in for Microsoft Outlook - Video Network tab contain the same prefix information. If Recording and Streaming are enabled in the Conference Profile, this number is used as part of the recording file name.</conference></mcu>	Displayed as the IP dial in number in the Access Number section of the Gathering Slide.			
Audio Access Number	ISDN/PSTN dial-in number. Up to two numbers are supported.	Displayed as the ISDN/PSTN dial-in number in the Access Number section of the Gathering Slide.			
Streaming recording link	Enables the recording of the conference to the Polycom RSS using the recording link. Enables streaming of the recording of the conference from the Polycom RSS.	If recording is enabled, a REC indicator is displayed in the top left corner of the slide.			

Connecting to a Conference

Participants can connect to the conference in the following ways:

- Participants with Polycom CMA/RealPresence Desktop™ or a Microsoft Office Communicator client running on their PCs can click on a link in the meeting invitation to connect to the meeting.
- Participants with a HDX or a room system will receive a prompt from the endpoint's calendaring system along with a button that can be clicked in order to connect.

Participants with endpoints that are not calendaring-enabled can connect to the meeting by dialing the meeting number manually.

Participants outside the office or using PSTN or mobile phones, can use the dial in number in the
meeting invitation to manually dial in to the meeting.

Collaboration Server Standalone Deployment

When using a single Collaboration Server in a standalone deployment, connection is via an Ad Hoc Entry Queue. The meeting is started when the first participant connects to the Collaboration Server.

When the first participant connects, a conference is created and named according to the information contained in the dial string. Subsequent participants connecting with the same dial string are routed from the Ad Hoc Entry Queue to the conference.

After the conference has been created the **Conference Name**, **Organizer**, **Time**, **Duration** and **Password** (if enabled) are retrieved from the conference parameters for display during the Gathering Phase.

Collaboration Server and Polycom RealPresence DMA System Deployment

In a RealPresence DMA system deployment a Virtual Meeting Room is activated when the first participant connects to the RealPresence DMA system. The RealPresence DMA system receives the dial string to activate a Virtual Meeting Room on the Collaboration Server.

The RealPresence DMA system uses the Meeting ID contained in the dial-in string to access meeting information stored in the Exchange Server database.

When the meeting information is found on the Exchange Server, the Conference Name, Organizer, Time, Duration and Password (if enabled) are retrieved from the Exchange Server database for display during the Gathering Phase.



If enabled, automatically generated passwords are ignored.

For more information see Automatic Password Generation Flags.

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners. These additional services will help customers successfully design, deploy, optimize and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. For additional information and details please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Conference and Participant Monitoring

You can monitor ongoing conferences and perform various operations while conferences are running. Three levels of monitoring are available with the Collaboration Server:

- General Monitoring You can monitor the general status of all ongoing conferences and their participants in the main window.
- Conference Level Monitoring You can view additional information regarding a specific conference and modify its parameters if required, using the Conference Properties option.
- Participant Level Monitoring You can view detailed information on the participant's status, using the Participant Properties option.
- The maximum number of participants in a conference:

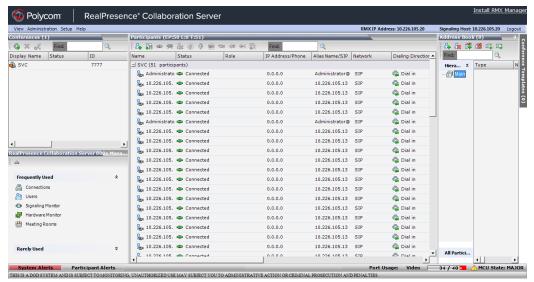


The following numbers are for media card assemblies with maximum resource capacities.

- RealPresence Collaboration Server (RMX) 1500 MPMx Mode: 360 (90 video).
- ➤ RealPresence Collaboration Server 1800 with 3 video accelerators: Up to 100 HD 720p 30 or 50 HD 1080p 25/30 fps.
- ➤ RealPresence Collaboration Server 1800 with 2 video accelerators: Up to 70 HD 720p 30 or 35 HD 1080p 25/30 fps.
- RealPresence Collaboration Server 1800 with 1 video accelerators: Up to 35 HD 720p 30 or 17 HD 1080p 25/30 fps.
- > RealPresence Collaboration Server (RMX) 2000 MPM Mode: 400 (80 video).
- > RealPresence Collaboration Server (RMX) 2000 MPM+ Mode: 800 (160 video).
- ➤ RealPresence Collaboration Server (RMX) 2000 MPMx Mode: 720 (180 video).
- RealPresence Collaboration Server (RMX) 4000 MPM+ Mode: 1600 (160 video).
- ➤ RealPresence Collaboration Server (RMX) 4000 MPMx Mode: 1440 (180 video)

General Monitoring

Users can monitor a conference or keep track of its participants and progress. For more information, see *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Monitoring Ongoing Conferences.



You can click the blinking **Participant Alerts** indication bar to view participants that require attention. For more information, see System and Participant Alerts.

Video Switching conferences appear with the HD (icon in the conferences list to differentiate between CP and VSW conferences.



Monitoring is done in the same way as for CP conferences.

Conference Level Monitoring

In addition to the general conference information that is displayed in the Conference list pane, you can view the details of the conference's current status and setup parameters, using the Conference Properties dialog box.

The tabs displayed in the Conference Properties dialog boxes are dependent on the Conferencing Mode, the participant authorization, and the Card Configuration Mode of the Collaboration Server — whether the Collaboration Server is configured with MPMx or MPMRx cards.

Conference monitoring - Tab list per conferencing mode and user

	Admi	n			Chair	person			Oper	ator		
Tab Name	СР	svc	Mixed	vsw	СР	svc	Mixed	vsw	СР	svc	Mixed	VSW
General	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Advanced	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gathering Settings	✓	×	×	✓	✓	×	×	✓	✓	×	×	✓
Video Quality	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Video Settings	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Audio Settings	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Customized Polling	✓	×	×	✓	*	×	×	×	✓	×	×	✓
Skins	✓	*	✓	×	✓	*	✓	×	✓	×	✓	×
IVR	✓	✓	✓	✓	×	*	×	×	✓	✓	✓	✓
Information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recording	✓	×	✓	✓	✓	*	✓	✓	✓	×	✓	✓
Site Names	✓	*	✓	×	✓	*	✓	×	✓	×	✓	×
Message Overlay	✓	×	×	*	✓	×	×	×	✓	×	×	×
Network Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Viewing the Properties of Ongoing CP and Mixed CP and SVC Conferences

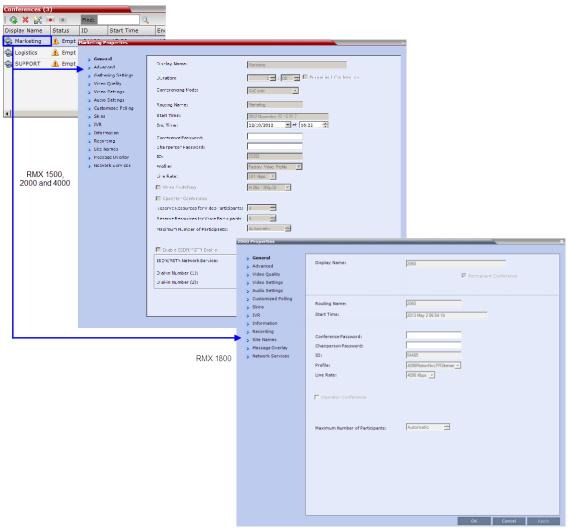
To view the parameters of an ongoing CP conference:

1 In the *Conference* list pane, double-click the **CP** conference or right-click the **CP** conference and then click **Conference Properties**.

The Conference Properties - General dialog box with the General tab opens.



RMX 1800 does not support VSW conferencing, ISDN/PSTN participants, and resource reservation. Therefore, all related fields do not appear in the *General* tab.



The following information is displayed in the General tab:

Conference Properties - General

Field	Description
Display Name	The Display Name is the conference name in native language and Unicode character sets to be displayed in the Collaboration Server Web Client. Note: This field is displayed in all tabs.
Duration	The expected duration of the conference using the format HH:MM. Note: This field is displayed in all tabs.
Permanent Conference	Indicates whether the conference is set as a Permanent Conference, with no pre-determined End Time. This conference continues until it is terminated by an administrator, operator or chairperson. Note: This field is displayed in all tabs.

Conference Properties - General

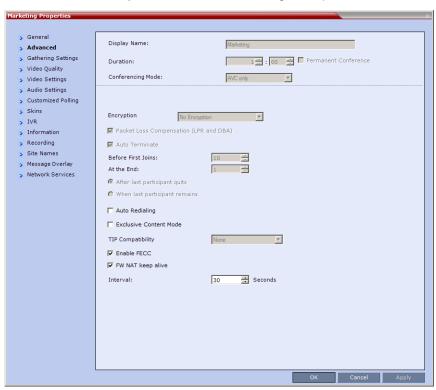
Field	Description
Routing Name	The ASCII name of the conference. It can be used by H.323 and SIP participants for dialing in directly to the conference. It is used to register the conference in the gatekeeper and the SIP server.
Conferencing Mode	The conferencing mode set for the conference: CP, VSW, SVC only or CP and SVC.
Start Time	The time the conference started.
End Time	The expected conference end time. Note: This field is not shown when the conference is set as a Permanent Conference.
Conference Password	A numeric password for participants to access the conference.
Chairperson Password	A numeric password used by participants to identify themselves as the conference chairperson.
ID	The conference ID.
Profile	The name of the conference Profile from which conference parameters were taken.
Line Rate	The maximum transfer rate, in kilobytes per second (Kbps) of the call (video and audio streams).
Video Switching	When selected, the conference is running in a special conferencing mode which implies that all participants must connect at the same line rate and the video parameters are set according to the highest common parameters. Participants with endpoints not supporting the video parameters (such as the video protocol, resolution and frame rate) selected for the conference will connect as secondary (audio only). If HD 1080p is selected for the conference, endpoints that do not support HD 1080p resolution are connected as Secondary (Audio Only) participants.
	Video layout changes are not enabled during a conference.
	Note: Video Switching conferencing mode is unavailable to ISDN participants. For more information, see Video Switching (VSW) Conferencing.
Reserve Resources for Video Participants	Displays the number of video participants for which the system reserved resources. Default: 0 participants.
Reserve Resources for Audio Participants	Displays the number of audio participants for which the system reserved resources. Default: 0 participants.
Max Number of Participants	Indicates the total number of participants that can be connected to the conference. The Automatic setting indicates the maximum number of participants that can be connected to the MCU according to resource availability.

Conference Properties - General

Field	Description
Enable ISDN/PSTN Network Service	When selected, ISDN/PSTN participants can dial into the conference.
ISDN/PSTN Network Service	When the Enable ISDN/PSTN Network Service is selected, displays the default Network Service.
Dial-in Number (1)	Displays the conference dial in number.
Dial-in Number (2)	Displays the conference dial in number.

2 Click the Advanced tab.

The Conference Properties - Advanced dialog box opens.



3 The following information is displayed in the Advanced tab:

Conference Properties - Advanced Parameters

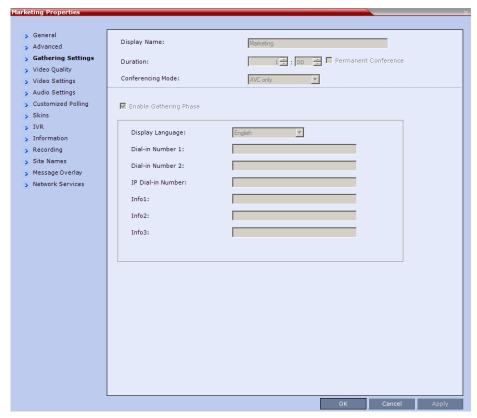
Field/Option	Description
Encryption	Indicates whether the conference is encrypted.
Packet Loss Compensation (LPR and DBA)	Indicates wether Packet Loss Compensation (LPR and DBA) is enabled for the conference.

Conference Properties - Advanced Parameters

Field/Option	Description	
Auto Terminate	When selected, indicates that the MCU will automatically terminate the conference when Before First Joins , At the End-After Last Quits and At the End - When Last Participant Remains parameters apply.	
Auto Redialing	Indicates whether dial-out participants are automatically (when selected) or manually (when cleared) connected to the conference. This option is disabled in mixed CP and SVC conferences.	
Exclusive Content Mode	When selected, Content is limited to one participant.	
TIP Compatibility	Indicates the TIP Compatibility mode implemented for the conference, when the environment implements the Collaboration Server and Cisco Telepresence Systems (CTS) Integration solution. None Video Only Video & Content Prefer TIP For more information, see Collaboration With Cisco's Telepresence Interoperability Protocol (TIP).	
Enable FECC	When selected, Far End Camera Control is enabled.	
FW NAT Keep Alive	When selected, sends a FW NAT Keep Alive message at specific Intervals for the RTP, UDP and BFCP channels. The interval specifies how often a FW NAT Keep Alive message is sent. For more information, see RealPresence Collaboration Server (RMX) Network Port Usage.	

4 Click the **Gathering Settings** tab.

The Conference Properties - Gathering Settings dialog box opens.



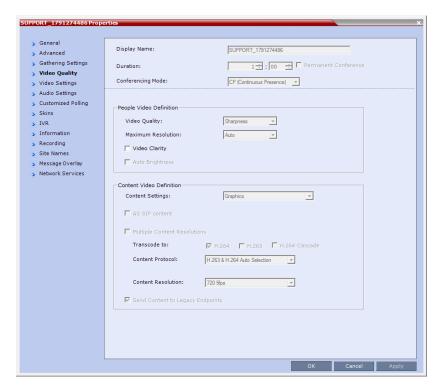
The following information is displayed:

Profile - Gathering Settings

Field/Options	Description
Enable Gathering	Indicates whether the Gathering Phase has been enabled.
Display Language	Indicates the language of the Gathering Slide field headings. Note: When working with the Polycom Conferencing Add-in for Microsoft Outlook, the language selected should match the language selected for the conference in the Polycom Conferencing Add-in for Microsoft Outlook to ensure that the Gathering Phase slide displays correctly.
Access Number 1	Indicates the ISDN or PSTN number(s) to call to connect to the conference.
Access Number 2	Note: The numbers entered must be verified as the actual Access Numbers.
Info 1	Additional information to be displayed during the Gathering Phase.
Info 2	_
Info 3	

5 Click the Video Quality tab.

The Conference Properties - Video Quality dialog box opens.



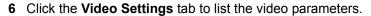
The following information is displayed:

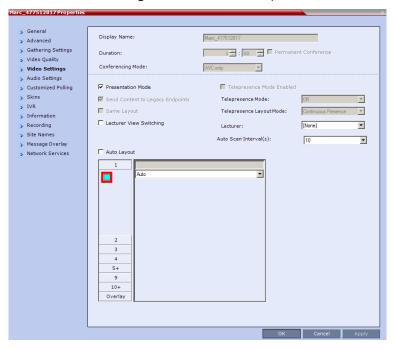
Conference Properties - Video Quality Parameters

Field/Option	Description	
People Video Definition		
Video Quality	Indicates the resolution and frame rate that determine the video quality set for the conference. Possible settings are: Motion or Sharpness . For more information, see Video Resolutions in AVC-based CP Conferencing.	
Maximum Resolution	Indicates the <i>Maximum Resolution</i> setting for the conference. • Auto (default) - indicates that the Maximum Resolution is selected in the Resolution Configuration dialog box. The Maximum Resolution settings for conferences and participants cannot be changed during an ongoing conference.	
Video Clarity™	Indicates if Video Clarity is enabled for the conference.	
Auto Brightness	Indicates if Auto Brightness is selected for the conference. Note: When Auto Brightness is enabled, color changes may be observed in computer-based VGA Content sent by HDX endpoints through the People video channel.	

Conference Properties - Video Quality Parameters

Field/Option	Description
Content Video Definition	
AS-SIP	Indicates if AS-SIP is enabled for the conference. When selected, content is shared using the Multiple Resolutions mode and is not supported in any other Content sharing mode. For more information, see Enabling AS-SIP Content.
Multiple Content Resolutions	Indicates if Multiple Content Resolutions mode for content sharing is enabled. In this mode, content is shared in multiple streams, one for each video protocol: H.263 and H.264. This allows endpoints with different protocols to connect and disconnect without having to restart Content sharing in the middle of a conference. For more information, see Sharing Content Using Multiple Content Resolutions Mode.
Content Settings	Indicates the Content channel resolution set for the conference. Possible resolutions are: • Graphics – default mode • Hi-res Graphics – requiring a higher bit rate • Live Video – content channel is live video • Customized Content Rate - resolution is manually defined.
Content Protocol	Indicates the Content Protocol used for content sharing in Highest Common Content Sharing Mode. For more information, see Content Protocols.
Content Resolution	Indicates the Content Resolution and frame rate according to the selected Content Sharing Mode (Highest common Content or Multiple Resolution Contents) and the video protocol. For more information, see Defining Content Sharing Parameters for a Conference.
Send Content to Legacy Endpoints (CP only)	Indicates if the <i>Send Content to Legacy Endpoints</i> is enabled. If enabled, Content can be sent to H.323/SIP/ISDN endpoints that do not support H.239 Content (legacy endpoints) over the video (people) channel. For more information see Sending Content to Legacy Endpoints (AVC Only).





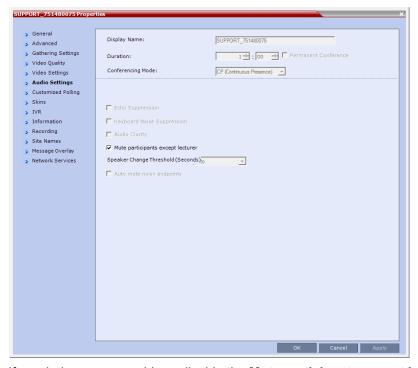
Conference Properties - Video Settings Parameters

Field	Description	
Presentation Mode	When checked, indicates that the Presentations Mode in This option is disabled in a mixed CP and SVC conference For more information, see Supplemental Conferencing	nce.
Lecturer View Switching	When checked, the Lecturer View Switching enables switching between the conference participants in the leteral This option is disabled in a mixed CP and SVC conference.	cturer video window.
Same Layout	When checked, forces the selected layout on all conference of Personal Layout option is disabled. This option is disabled in a mixed CP and SVC conference of the conference	
Auto Layout	When enabled, the system automatically selects the co the number of participants in the conference.	nference layout based on
Telepresence Mode Enabled	Indicates if the conference is running in Telepresence Mode.	These fields are enabled if the Collaboration
Telepresence Mode	Indicates the Telepresence Mode.	 Server has a Telepresence license
Telepresence Layout Mode	Indicates the layout of the Telepresence Mode.	installed. See Defining New Profiles.

Conference Properties - Video Settings Parameters

Field	Description
Lecturer	Indicates the name of the lecturer (if one is selected). Selecting a lecturer enables the Lecture Mode. This option is disabled in a mixed CP and SVC conference.
Auto Scan Interval(s)	The time interval, 10 - 300 seconds, that Auto Scan uses to cycle the display of participants that are not in the conference layout in the selected cell. This option is disabled in a mixed CP and SVC conference.
Video Layouts (graphic)	Indicates the currently selected video layout.

7 Click the Audio Settings tab to view the audio setting for the conference.



- 8 If needed, you can enable or disable the Mute participants except lecturer setting.
- **9 CP Only Conferences:** Click the C**ustomized Polling** tab to view and modify the customized polling for the conference.

All conference participants are listed in the left pane (**All Participants**) while the participants that are to be displayed in the Auto Scan enabled cell of the video layout are listed in the right pane (**Scanning Order**).

The dialog box buttons are summarized in the table below.

Customized Polling - Buttons

Button	Description
Add	Select a participant and click this button to add a the participant to the list of participants to be Auto Scanned. The participants name is removed from the All Participants pane.
Delete	Select a participant and click this button to delete the participant from the list of participants to be Auto Scanned. The participants name is moved back to the All Participants pane.
Add All	Add all participants to the list of participants to be Auto Scanned. All participants' names are removed from the All Participants pane.
Delete All	Delete all participant from the list of participants to be Auto Scanned. All participants' names are moved back to the All Participants pane.
Up	Select a participant and click this button to move the participant up in the Scanning Order.
Down	Select a participant and click this button to move the participant down in the Scanning Order.

10 Click Apply to confirm and keep the Conference Properties dialog box open.

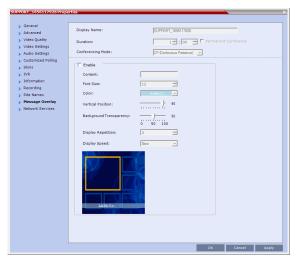
or

Click **OK** to confirm and return to the Collaboration Server Web Client main screen.

11 Click the **Skins** tab to view the skin selected for the conference.

You cannot select another skin during an ongoing conference.

- 12 Click the IVR tab to view the IVR settings.
- **13** Click the **Information** tab to view general information defined for the conference. Changes made to this information once the conference is running are not saved to the CDR.
- **14** Click the **Recording** tab to review the recording settings for the conference.
- **15** Click the **Site Names** tab to enable or disable the display of site names during the conference, and adjust the display properties.
- **16** Click the **Message Overlay** tab to send text messages to the conference participants during the conference, and adjust the display properties of the text messages.



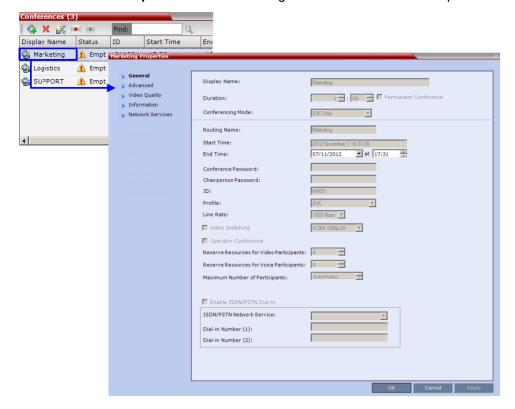
For more information, see Sending Text Messages During a Conference Using Message Overlay.

- 17 Click the **Network Services** tab to verify the SIP registration for the conference.
- 18 Click OK to close the Conference Properties dialog box.

Viewing the Properties of Ongoing SVC-based Conferences

To view the parameters of an ongoing SVC conference:

1 In the **Conference** list pane, double-click the SVC conference or right-click the SVC conference and then click **Conference Properties**.



The Conference Properties - General dialog box with the General tab opens.

2 The following information is displayed in the **General** tab:

Conference Properties - General Parameters

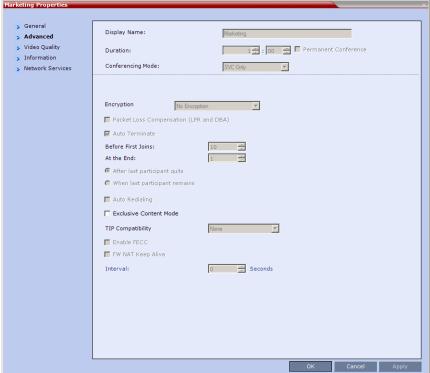
Field	Description
Display Name	The Display Name is the conference name in native language and Unicode character sets to be displayed in the Collaboration Server Web Client. Note: This field is displayed in all tabs.
Duration	The expected duration of the conference using the format HH:MM. Note: This field is displayed in all tabs.
Conferencing Mode	The conferencing mode for the conference.
Routing Name	The ASCII name of the conference. It can be used by H.323 and SIP participants for dialing in directly to the conference. It is used to register the conference in the gatekeeper and the SIP server.
Start Time	The time the conference started.
End Time	The expected conference end time.
Conference Password	Conference Password is not supported in SVC conferences.

Conference Properties - General Parameters

Field	Description
Chairperson Password	Chairperson Password is not supported in SVC conferences.
ID	The conference ID.
Profile	The name of the conference Profile from which conference parameters were taken.
Line Rate	The maximum transfer rate, in kilobytes per second (Kbps) of the call (video and audio streams).
Video Switching	Video Switching is not supported in SVC conferences.
Reserve Resources for Video Participants	Reserve Resources for Video Participants is not supported in SVC conferences.
Reserve Resources for Audio Participants	Reserve Resources for Audio Participants is not supported in SVC conferences.
Max Number of Participants	Indicates the total number of participants that can be connected to the conference. The Automatic setting indicates the maximum number of participants that can be connected to the MCU according to resource availability.
Enable ISDN/PSTN Network Service	ISDN/PSTN participants are not supported in SVC conferences.
ISDN/PSTN Network Service	ISDN/PSTN participants are not supported in SVC conferences.
Dial-in Number (1)	ISDN/PSTN participants are not supported in SVC conferences.
Dial-in Number (2)	ISDN/PSTN participants are not supported in SVC conferences.

3 Click the Advanced tab.

The Conference Properties - Advanced dialog box opens. Marketing Properties



4 The following information is displayed in the **Advanced** tab:

Conference Properties - Advanced Parameters

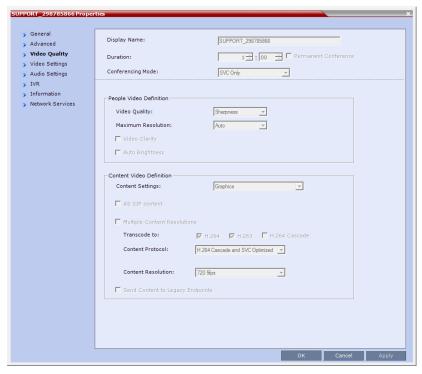
Field/Option	Description
Encryption	Indicates the Encryption setting for the conference.
Packet Loss Compensation (LPR and DBA)	Packet Loss Compensation is not supported in SVC conferences.
Auto Terminate	When selected, indicates that the MCU will automatically terminate the conference when Before First Joins, At the End-After Last Quits and At the End - When Last Participant Remains parameters apply.
Auto Redialing	Dial-out is not supported in SVC conferences.
Exclusive Content Mode	When selected, Content is limited to one participant.
TIP Compatibility	TIP Compatibility is not supported in SVC conferences.
Enable FECC	Far End Camera Control is not supported in SVC conferences.

Conference Properties - Advanced Parameters

Field/Option	Description
FW NAT Keep Alive	When selected, sends a FW NAT Keep Alive message at specific Intervals for the RTP, UDP and BFCP channels. The interval specifies how often a FW NAT Keep Alive message is sent. For more information, see RealPresence Collaboration Server (RMX) Network Port Usage.

5 Click the Video Quality tab.

The Conference Properties - Video Quality dialog box opens.



The following information is displayed:

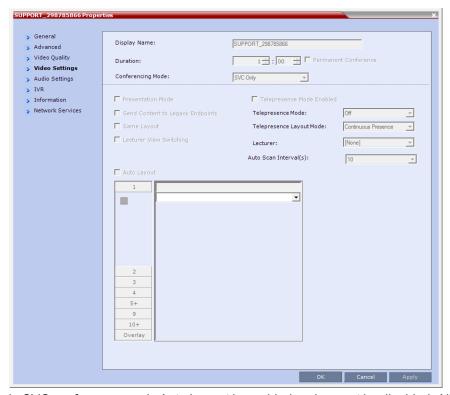
Conference Properties - Video Quality Parameters

Field/Option	Description	
People Video Definition	People Video Definition	
Video Quality	Indicates the resolution and frame rate that determine the video quality set for the conference. In <i>SVC conferencing</i> , only Sharpness is supported.	
Maximum Resolution	In SVC conferencing, this is always Auto (default) - The Maximum Resolution remains as selected in the Resolution Configuration dialog box.	
Video Clarity™	Video Clarity is not supported in SVC conferences.	
Auto Brightness	Auto Brightness is not supported in SVC conferences.	

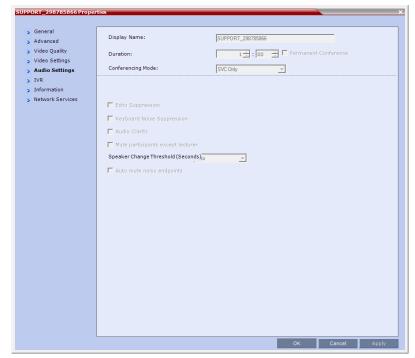
Conference Properties - Video Quality Parameters

Field/Option	Description
Content Video Defini	tion
AS-SIP	AS-SIP is not supported in SVC conferences.
Multiple Content Resolutions	Multiple Content Resolutions is not supported in SVC conferences.
Content Settings	In SVC conferencing, this is always set to Graphics
Content Protocol	In SVC conferencing this is always set to H.264 Cascade and SVC Optimized .
Content Resolution	Resolution is fixed in SVC conferences.

6 Click the Video Settings tab to view the video parameters defined for the conference.



In SVC conferences, only Auto Layout is enabled and cannot be disabled. All other video settings are disabled.



7 Click the Audio Settings tab to view the audio parameters defined for the conference.

In SVC conferences, all Audio Settings options are disabled.

- **8** Click the **Information** tab to view general information defined for the conference. Changes made to this information once the conference is running are not saved to the CDR.
- 9 Click **OK** to close the **Conference Properties** dialog box.

Monitoring of Operator Conferences and Participants Requiring Assistance (CP and Mixed CP and SVC Conferences)

Operator conferences are monitored in the same way as standard ongoing conferences.

Each Operator conference includes at least one participant - the Operator.



You can view the properties of the Operator conference by double-clicking the conference entry in the Conferences list or by right-clicking the conference entry and selecting **Conference Properties**. For more information, see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, Conference Level Monitoring.

Requesting Help

A participant can request help using the appropriate DTMF code from his/her touch tone telephone or the endpoint's DTMF input device. The participant can request Individual Assistance (default DTMF code *0) or Conference Assistance (default DTMF code 00).

Participants in Entry Queues who failed to enter the correct destination conference ID or the conference password will wait for operator assistance (provided that an Operator conference is active).

When requiring or requesting operator assistance, the Collaboration Server management application displays the following:



- The participant's connection Status changes, reflecting the help request. For details, see Participants
 List Status Column Icons and Indications.
- The conference status changes and it is displayed with the exclamation point icon and the status Awaiting Operator.
- The appropriate voice message is played to the relevant participants indicating that assistance will be provided shortly.

The following icons and statuses are displayed in the **Participant Status** column:

Participants List Status Column Icons and Indications

Icon	Status indication	Description
a	Awaiting Individual Assistance	The participant has requested the operator's assistance for himself/herself.
<u> </u>	Awaiting Conference Assistance	The participant has requested the operator's assistance for the conference. Usually this means that the operator is requested to join the conference.

When the Operator moves the participant to the Operator conference for individual assistance the participant Status indications are cleared.

Request to Speak

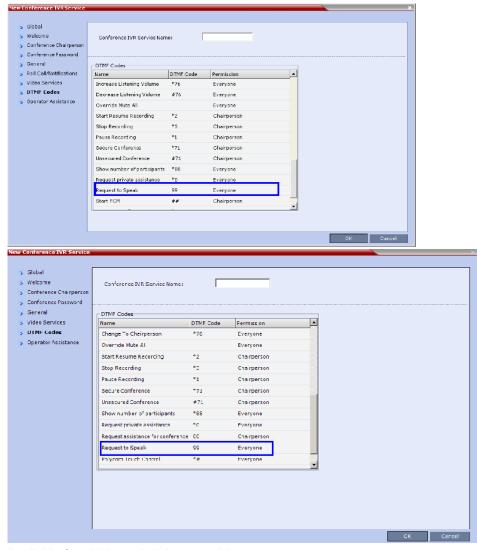
Participants that were muted by the conference organizer/system operator can indicate that they want to be unmuted by entering the appropriate DTMF code.

An icon is displayed in the **Role** column of the **Participants** list for 30 seconds.



Request to Speak is:

Activated when the participant enters the appropriate DTMF code (default: 99).
 The DTMF code can be modified in the conference IVR Service Properties - DTMF Codes dialog box.

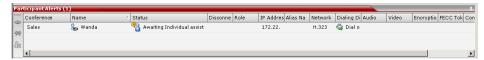


- Available for dial-in and dial-out participants.
- A participant can request to speak more than once during the conference.
- Supported in all conference types.

- Supported in H.323 and SIP environments.
- The duration of the icon display cannot be modified.

Participant Alerts List

The Participant Alerts list contains all the participants who are currently waiting for operator assistance.



Participants are automatically added to the Participants Alerts list in the following circumstances:

- The participant fails to connect to the conference by entering the wrong conference ID or conference
 password and waits for the operator's assistance.
- The participant requests Operator's Assistance during the ongoing conference.

This list is used as reference only. Participants can be assisted and moved to the Operator conference or the destination conference only from the **Participants** list of the Entry Queues or ongoing conference where they are awaiting assistance.

The participants are automatically removed from the **Participant Alerts** list when moved to any conference (including the Operator conference).

Participant Level Monitoring

In addition to conference information, you can view detailed information regarding the status and parameters of each listed participant, using the **Participant Properties** dialog box. Participant properties can be displayed for all participants currently connected to a conference and for defined participants that have been disconnected.



Properties differ for IP and ISDN/PSTN participants.

SIP SVC-based participant properties are similar to SIP AVC-based participant properties.

The table below lists the tabs in the **Participant Properties** dialog box, as viewed by each user type, for each participant connection types.

Participant monitoring - Tab list per participant connection type and user

	Admin		Chairperson		Operator	
Tab Name	AVC H.323	AVC/SVC SIP	AVC H.323	AVC/SVC SIP	AVC H.323	AVC/SVC SIP
General	✓	✓	✓	✓	✓	✓
Advanced	✓	✓	×	×	✓	✓
Information	✓	✓	✓	✓	✓	×
Media Sources	✓	✓	✓	✓	✓	✓
H.245	✓	×	×	×	✓	×

Participant monitoring - Tab list per participant connection type and user

	Admin		Chairperson		Operator	
Tab Name	AVC H.323	AVC/SVC SIP	AVC H.323	AVC/SVC SIP	AVC H.323	AVC/SVC SIP
SDP	×	✓	×	×	×	✓
Connection Status	✓	✓	×	*	✓	✓
Channel Status	✓	✓	×	×	✓	✓
Channel Status - Advanced	✓	✓	*	*	×	×
Gatekeeper Status	✓	✓	×	×	×	×
Call Admission Control	×	×	×	×	×	×

Viewing the Properties of Participants

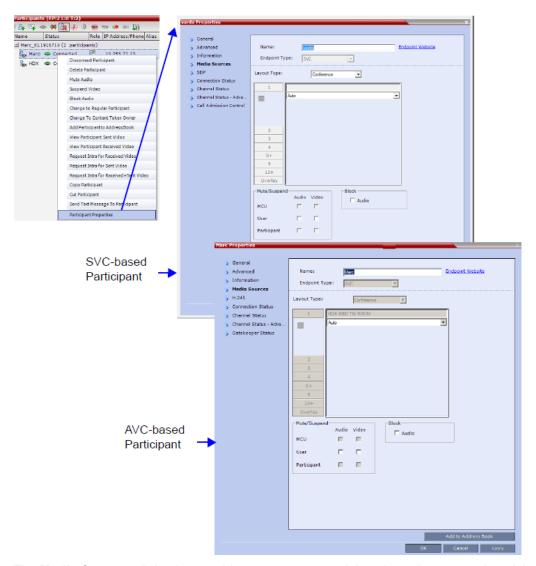
To view the participant Properties:

» In the **Participant List** pane double-click the participant entry. Alternatively, right-click a participant and then click **Participant Properties**.

The **Participant Properties** dialog box opens, displaying the last opened tab.



Media Sources properties are not available for SVC participants.



The **Media Sources** dialog box enables you to mute participant's audio, suspend participant's video transmission and select a personal Video Layout for the participant.



For ISDN/PSTN participants, only the following tabs are displayed in the **Participant Properties** dialog box:

- · General, Advanced, Information
- · Media Sources
- · Connection Status
- · Channel Status

The **General**, **Advanced** and **Information** tabs include the same properties for new and defined participants. For more information, see Adding a New participant to the Address Book Directly.

Monitoring IP Participants

The following parameters are displayed for an IP participant.

Participant Properties - Media Sources Parameters

Field	Description
Name	Indicates the participant's name. Note: This field is displayed in all tabs.
Endpoint Website (link)	Click the Endpoint Website hyperlink to connect to the internal website of the participant's endpoint. It enables you to perform administrative, configuration and troubleshooting activities on the endpoint.
	The connection is available only if the IP address of the endpoint's internal site is filled in the Website IP Address field in the Participant Properties - General dialog box.
	Note: This field is displayed in all tabs (excluding ISDN/PSTN participants). Endpoint Website hyperlinks are not supported when the Collaboration Server is in Ultra Secure Mode. For more information see Ultra Secure Mode.
Endpoint Type	Indicates whether the participant is using an AVC-based or SVC-based endpoint. Fields, tabs and options are enabled or disabled according to the endpoint type. Note: This field is displayed in all tabs.
Layout Type	Indicates whether the video layout currently viewed by the participant is the Conference or Personal Layout. If Personal Layout is selected, you can select a Video Layout that will be viewed only by this participant.
Video Layout	Indicates the video layout currently viewed by the participant. When Personal Layout is selected in the Layout Type you can force participants to the video windows in a layout that is specific to the participant. For more information, see <i>Polycom RealPresence Collaboration Server (RMX)</i> 1500/1800/2000/4000 Getting Started Guide, Changing the Video Layout of a Conference (AVC-Based CP and Mixed CP and SVC Conferences).
Mute/Suspend	Indicates if the endpoint's audio and/or video channels have been muted/suspended. The entity that initiated audio mute or video suspend is also indicated.
	 MCU – Audio or Video channel has been muted/suspended by the MCU.
	User – Channels have been muted/suspended by the Collaboration Server user.
	 Participant – Channels have been muted/suspended by the participant from the endpoint.
	You can also cancel or perform mute and suspend operation using these check boxes. Note: If the participant muted his/her audio channel, the system displays the mute icon only for H.323. This icon is not displayed for SIP participant due to SIP standard limitation.
Block	When checked, the audio transmission from the conference to the participant's endpoint is blocked, but the participant will still be heard by other participants.

¹ Click the **Connection Status** tab to view the connection status, and if disconnected the cause of the disconnection.



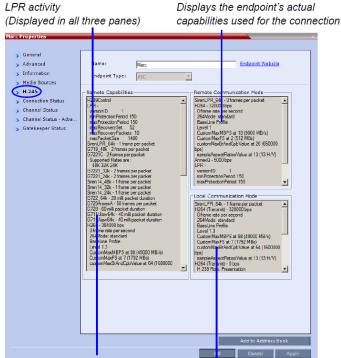
This dialog box is the same for AVC-based and SVC-based participants.

The following parameters are displayed:

Participant Properties - Connection Status Parameters

Field	Description
Participant Status	
Status	Indicates the connection status of the participant.
Connection Time	The date and time the participant connected to the conference. Note: The time format is derived from the MCU's operating system time format.
Disconnection Time	The date and time the defined participant disconnected from the conference.
Connection Retries Left	Indicates the number of retries left for the system to connect defined participant to the conference.
Call Disconnection Cause	Displays the cause for the defined participant's disconnection from the conference. See Conference and Participant Monitoring.
Video Disconnection Cause	Displays the cause the video channel could not be connected. For more information, see Appendix A - Disconnection Causes.
Possible Solution	In some cases, a possible solution is indicated to the cause of the video disconnection.

2 Click the H.245 (H.323) or SDP (SIP) tab during or after the participant's connection process to view information that can help in resolving connection issues.



H.323 Participant (AVC-based)

List's the endpoint's capabilities as retrieved from the remote site

Displays the MCU's capabilities used for connection with the participant

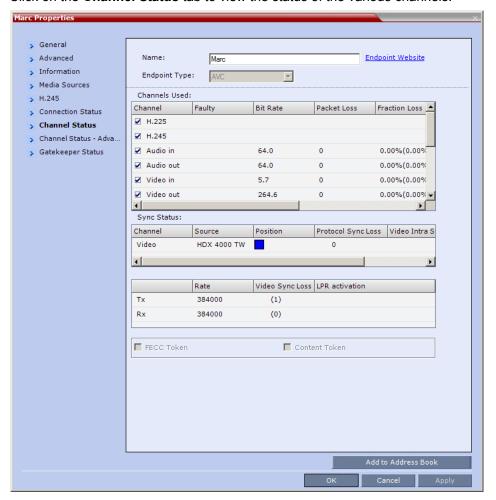


SIP Participant (AVC-based and SVC-based)

Participant Properties - H.245/SDP Parameters

Field	Description
Remote Capabilities	Lists the participant's capabilities as declared by the endpoint.
Remote Communication Mode	Displays the actual capabilities used by the endpoint when establishing the connection with the MCU (Endpoint to MCU).
Local Communication Mode	Displays the actual capabilities used by the MCU when establishing the connection with the participant's endpoint (MCU to Endpoint).

3 Click on the Channel Status tab to view the status of the various channels.



The following parameters are displayed:

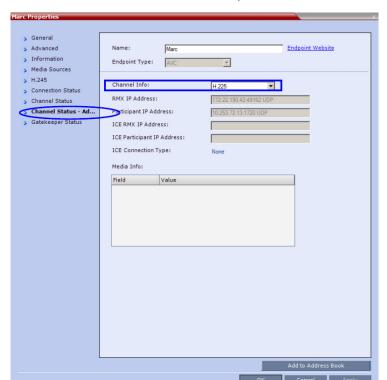
Participant Properties - Channel Status Parameters

Field	Description
Channels Used	When checked, indicates the channel type used by the participant to connect to the conference: Incoming channels are endpoint to MCU, Outgoing channels are from MCU to endpoint. Channels:
	H.225/Signaling - The call-signaling channel. H.245/CDD. The Control shaped.
	H.245/SDP - The Control channel. Audio in - Incoming audio channel.
	Addie in Theoring addie Granner
	Additional Categoring additional Control
	video in miconing video chamion
	Video out - Outgoing video channel Content in U 220/Recoller Content conferences
	Content in - H.239/People+Content conferences Content out - H.239/People - Content conferences
	Content out - H.239/People+Content conferences EECC in The incoming EECC channel in open.
	FECC out. The outraing FECC channel is open. FECC out. The outraing FECC channel is open. FECC out. The outraing FECC channel is open.
	FECC out - The outgoing FECC channel is open. Columns:
	Columns:
	 Faulty – A red exclamation point indicates a faulty channel condition. This is a real-time indication; when resolved the indication disappears. An exclamation point indicates that further investigation may be required using additional parameters displayed in the Advanced Channel Status tab.
	• Bit Rate – The actual transfer rate for the channel. When channel is inactive, bit rate value is 0. For example, if the participant is connected without video, the bit rate for the video channel is 0.
	Note: The CTS Audio Auxiliary channel is used only for Content. In all other cases, the bit rate shown in this column for this channel is 0.
	 Packet Loss – The accumulated count of all packets that are missing according to the RTCP report since the channel was opened. This field is relevant only during the connection stage and does not display faulty indications.
	• Fraction Loss (Peak) – The ratio between the number of lost packets and the total number of transmitted packets since the last RTCP report. Peak (in parentheses) indicates the highest ratio recorded since the channel was opened.
	• Number of Packets – The number of received or transmitted packets since the channel has opened. This field does not cause the display of the faulty indicator.
	• Jitter (Peak) – Displays the network jitter (the deviation in time between the packets) as reported in the last RTCP report (in milliseconds). Peak (in parentheses) reflects the maximum network jitter since the channel was opened.
	 Latency – Indicates the time it takes a packet to travel from one end to another in milliseconds (derived from the RTCP report).
	High latency value may indicate that there is a problem in the network, or that the endpoint is sending an incorrect RTCP values.

Participant Properties - Channel Status Parameters

Field	Description
Sync Status	 Channel - The channel type: Video or Content. Source - The name of the participant currently viewed by this participant. Position - The video layout position indicating the place of each participant as they appear in a conference. Protocol Sync Loss - Indicates whether the system was able to synchronize the bits order according to the selected video protocol. Video Intra Sync - Indicates whether the synchronization on a video Intra frame was successful. Video Resolution - The video resolution of the participant.
Rx - Rate	The received line rate.
Tx - Rate	The transmitted line rate.
Tx - Video Sync Loss	When checked, indicates a video synchronization problem in the outgoing channel from the MCU. The counter indicates the sync-loss count.
Rx - Video Sync Loss	When checked, indicates a video synchronization problem in the incoming channel from the endpoint. The counter indicates the sync-loss count.
Tx - LPR Activation	When checked, indicates LPR activation in the outgoing channel.
Rx - LPR Activation	When checked, indicates LPR activation in the incoming channel.
FECC Token	When checked, indicates that the participant is the holder of the FECC Token.
Content Token	When checked, indicates that the participant is the holder of the Content Token.

4 Click the **Channel Status Advanced** tab to view additional information for selected audio and video channels.



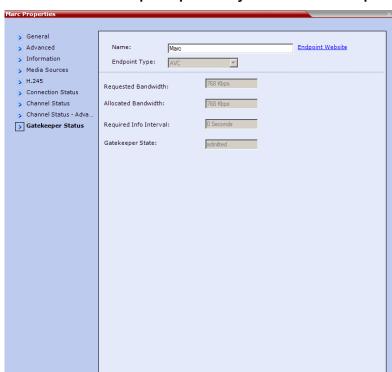
In the **Channel Status - Advanced** tab, channels can be selected for viewing additional information:

Participant Properties - Channel Status Advanced Parameters

Field	Description
Channel Info	Select a channel to view its information: H.225 H.245 Audio in Audio out Video in Video out Content in SIP BFCP TCP
RMX IP Address	The IP address and the transport protocol (TCP/UDP) of the MCU to which the participant is connected and the port number allocated to the participant incoming media stream on the MCU side.
Participant IP Address	The IP address and the transport protocol (TCP/UDP) of the participant and the port number allocated to the media stream on the participant side.

Participant Properties - Channel Status Advanced Parameters

Field	Description	
ICE RealPresence Collaboration Server (RMX) 1500/1800/2000/400 0 IP Address	The IP address, port number, and transport protocol of the MCU used to pass through the media when ICE is functional. See Participant Properties - ICE Connection Parameters.	
ICE Participant IP Address	The IP address, port number, and transport protocol of the endpoint used to pass through the media when ICE is functional. See Monitoring the Participant Connection in ICE Environment.	
ICE Connection Type	 Indicates the type of connection between the Collaboration Server and the participant in the ICE environment: Local (or Host) - The endpoint (Remote) is on the same network as the Collaboration Server and the media connection is direct, using local addresses. Relay - Media between the Collaboration Server and the participant passes through a media relay server. Firewall - Media connection between the Collaboration Server and the participant is done using their external IP addresses (the IP addresses as seen outside of the local network). 	
Media Info	This table provides information about the audio and video parameters, such as video algorithm, resolution, etc. For more information, see Appendix E - Participant Properties Advanced Channel Information.	
RTP Statistics	This information may indicate problems with the network which can affect the audio and video quality. For more information, see Appendix E - Participant Properties Advanced Channel Information.	



5 For H.323 AVC-based participants only - Click the Gatekeeper Status tab to view its parameters.

Participant Properties - Gatekeeper Status Parameters

Field	Description	
Requested Bandwidth	The bandwidth requested by the MCU from the gatekeeper.	
Allocated Bandwidth	The actual bandwidth allocated by the gatekeeper to the MCU.	
Required Info Interval	Indicates the interval, in seconds, between registration messages that the MCU sends to the gatekeeper to indicate that it is still connected.	
Gatekeeper State	 Indicates the status of the participant's registration with the gatekeeper and the bandwidth allocated to the participant. The following statuses may be displayed: ARQ – Admission Request - Indicates that the participant has requested the gatekeeper to allocate the required bandwidth on the LAN. Admitted – Indicates that the gatekeeper has allocated the required bandwidth to the participant. DRQ – Disengage Request – The endpoint informs the gatekeeper that the connection to the conference is terminated and requests to disconnect the call and free the resources. None – Indicates that there is no connection to the gatekeeper. 	

6 For SIP AVC-based and SVC-based participants - Click the **Call Admission Control** tab to view its parameters.



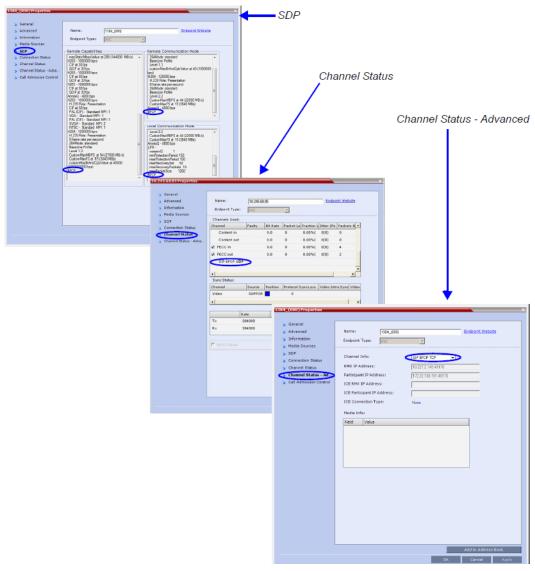
Participant Properties - Gatekeeper Status Parameters

Field	Description	
Requested Bandwidth	The bandwidth requested by the MCU from the SIP server.	
Allocated Bandwidth	The actual bandwidth allocated by the SIP server to the MCU.	

Monitoring SIP BFCP Content

In the SIP Participant Properties dialog box, BFCP status information appears in:

- All three panes of the SDP tab.
- The Channel Status tab.
- The Channel Status Advanced tab.



For more information see Participant Level Monitoring.

Detecting SIP Endpoint Disconnection

When an abnormal disconnection of SIP endpoints occurs because of network problems or client application failures, SIP endpoints remain connected to the conference causing connection disruptions. For example, the video freezes in the layout or blocks content for SIP endpoints when a quick re-connection is performed. It can take several minutes to detect the SIP endpoint disconnection using the SIP standard behavior.

In a normal SIP video call, audio and video (RTP and RTCP) messages are sent from the endpoints to the MCU to detect the signaling of connected endpoints. Conversely, SVC endpoints might not send video RTP messages to the MCU when a participant is not displayed in the video layout of any of the participants in the conference. For SVC endpoints, the MCU will only verify audio RTP and RTCP messages and video RTCP messages. Video RTP messages will not be checked.

To detect the disconnection of SIP endpoints in a reasonable amount of time, a new system flag can be defined to specify the amount of time that the MCU should wait for an RTCP or RTP message from the SIP endpoint before the endpoint starts the disconnection process. The system default value is automatically set to 20 seconds.

The system flag, **DETECT_SIP_EP_DISCONNECT_TIMER**, contains the amount of time in seconds to wait for an RTCP or RTP message to be received from the endpoint. When the time that was set in the system flag has elapsed and no RTCP or RTP audio or video message has been received on either the audio or the video channel, the MCU disconnects the SIP endpoint from the conference. A CDR event record is created with a Call Disconnection Cause of SIP remote stopped responding.

The Microsoft Lync add-in endpoint opens audio and content channels. Lync endpoints can send RTCP/RTP messages and empty RTP audio messages. When the time that was set in the system flag has elapsed and no RTCP or RTP message has been received on the audio channel, the MCU disconnects the endpoint from the conference.

SIP audio only endpoints use the audio channel only. When the time that was set in the system flag has elapsed and no RTCP or RTP message has been received on the audio channel, the MCU disconnects the SIP audio endpoint from the conference.

Configuring the System Flag

When you want to change the system default value of 20 seconds, the system flag, **DETECT_SIP_EP_DISCONNECT_TIMER**, can be manually added to the System Flags configuration to detect the disconnection of SIP endpoints. For more information see Manually Adding and Deleting System Flags.

The value range is from 0 to 300 seconds. When the value is set between 0 and 14, the feature is disabled and SIP endpoints are not detected for disconnection. When the value is set between 15 and 300, the feature is enabled.

Monitoring ISDN/PSTN Participants

Using the **Participant Properties** dialog box, you can monitor and verify the properties of an ISDN/PSTN participant. The dialog box's tabs contain information that is relevant to the participant's status only while the conference is running and is used to monitor the participant's status when connection problems occur.



Maximum line rate at which ISDN endpoints can connect to a conference is 768 kbps.

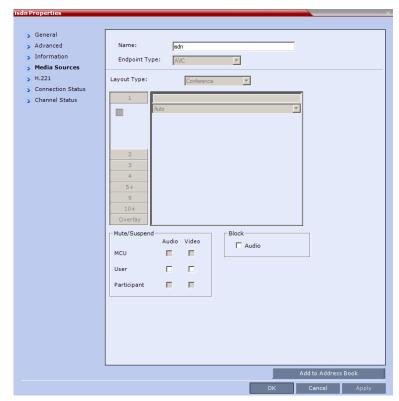
The table below lists the audio algorithms that are supported for ISDN participants according to their connection bit rate

Supported Audio Algorithms vs Bit Rate

	Bit Rate		
	96Kbps (and Lower)	128Kbps – 192Kbps	256Kbps (and Higher)
Audio Algorithm	G722.1 16K	G722.1 C 32K	G722.1 C 48K
	G722.1 C 24K	G722.1 C 24K	G722.1 C 32K
	Siren14 24K	Siren14 32K	G722.1 C 24K
	G722 48K	Siren14 24K	Siren14 48K
	G722 56K	G722.1 32K	Siren14 32K
	G722 64K	G722.1 24K	Siren14 24K
	G711 56K	G722 48K	G722.1 32K
	G711 64K	G722 56K	G722.1 24K
		G722 64K	G722.1 16K
		G711 56K	G722 48K
		G711 64K	G722 56K
			G722 64K
			G711 56K
			G711 64K

To view the participant properties during a conference:

1 In the Participants list, right click the desired participant and select Participant Properties.

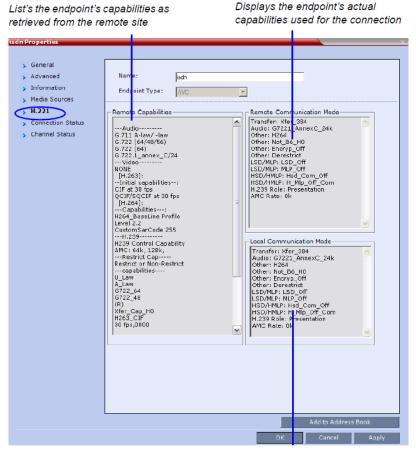


The Participant Properties - Media Sources dialog box is displayed.

ISDN/PSTN Participant Properties - Media Sources

Field	Description	
Mute/Suspend	Indicates if the endpoint's audio and/or video channels from the endpoint have been muted/suspended.	
	The entity that initiated audio mute or video suspend is also indicated.	
	 MCU – Audio or Video channel has been muted/suspended by the MCU. 	
	• User – Channels have been muted/suspended by the Collaboration Server user.	
	 Participant – Channels have been muted/suspended by the participant from the endpoint. 	
	You can also cancel or perform mute and suspend operation using these check boxes.	
Block (Audio)	When checked, the audio transmission from the conference to the participant's endpoint is blocked, but the participant will still be heard by other participants.	

2 Click the **H.221** tab to view additional information that can help to resolve connection issues.



Displays the MCU's capabilities used for connection with the participant

Participant Properties - H.221 Parameters

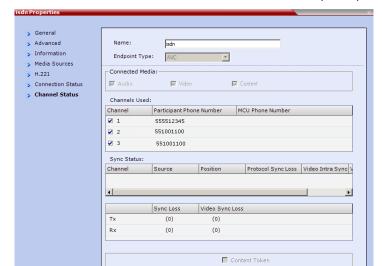
Field	Description
Remote Capabilities	Lists the participant's capabilities as declared by the endpoint.
Remote Communication Mode	Displays the actual capabilities used by the endpoint when establishing the connection with the MCU (Endpoint to MCU).
Local Communication Mode	Displays the actual capabilities used by the MCU when establishing the connection with the participant's endpoint (MCU to Endpoint).

3 Click the **Connection Status** tab to view general information regarding the participant connection and disconnection causes of the participant to the conference.



ISDN/PSTN Participant Properties - Connection Status

Field	Description	
Status	Indicates the connection status of the participant to the conference. If there is a problem, the appropriate status is displayed, for example, Disconnected.	
Connection Time	The date and time the participant connected to the conference.	
Disconnection Time	The date and time the participant was disconnected from the conference.	
Connection Retries Left	Indicates the number of retries left for the system to connect the participant to the conference.	
Call Disconnection Cause	For a full list of Disconnection Causes, Appendix A - Disconnection Causes.	

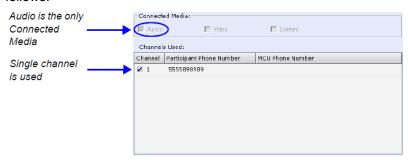


4 Click the **Channel Status** tab to view the status of a participant's channels.

ISDN/PSTN Participant Properties - Channel Status

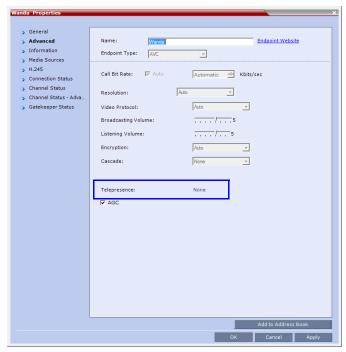
Field	Description
Connected Media	Indicates if the participant is connected with Audio, Video and Content media channels.
Channels Used	 Channel – Indicates the channel used by the participants and whether the channel is connected (indicated with a check mark) or disconnected.
	 Participant Phone Number – In a dial-in connection, indicates the participant's CLI (Calling Line Identification) as identified by the MCU.
	In a dial-out connection, indicates the participant's phone number dialed by the MCU for each channel.
	 MCU Phone Number – In a dial-in connection, indicates the MCU number dialed by the participant.
	In a dial-out connection, indicates the MCU (CLI) number as seen by the participant. This is the number entered in the MCU Number field in the Network Service.
Tx - Video Sync Loss	When checked, indicates a video synchronization problem in the outgoing channel from the MCU.
	The counter indicates the sync-loss count.
Rx - Video Sync Loss	When checked, indicates a video synchronization problem in the incoming channel from the endpoint.
	The counter indicates the sync-loss count.
Content Token	A check mark indicates that the participant is the current holder of the Content Token.

The **Connected Media** and **Channels Used** fields of an **Audio Only** participant are displayed as follows:



Monitoring Telepresence Participant Properties

A **Telepresence** status indicator is displayed in the **Participant Properties - Advanced** tab when monitoring conference participants.



The Telepresence mode of the participant is indicated:

- RPX the participant's endpoint is transmitting 4:3 video format.
- TPX the participant's endpoint is transmitting 16:9 video format.
- None the participant's endpoint is neither RPX nor TPX.

Recording Conferences



Conference recording is not available in SVC Conferencing Mode.

Conferences running on the Collaboration Server can be recorded using a Polycom® RSS™ Recording and Streaming Server (RSS).

The recording system can be installed at the same site as the conferencing MCU or at a remote site. Several MCU's can share the same recording system.

Recording conferences is enabled via a Recording Link, which is a dial-out connection from the conference to the recording system.

Recording can start automatically, when the first participant connects to a conference, or on request, when the Collaboration Server user or conference chairperson initiates it.

Multiple Recording Links may be defined.

Conference Recording Links can be associated on the Collaboration Server with Virtual Recording Rooms (VRR), created and saved on the Polycom® RSS™ 4000 Version 8.5 Recording and Streaming Server (RSS).

Each Recording Link defined on the Collaboration Server can be given a descriptive name and can be associated with one VRR saved on the Polycom RSS 4000.

The following guidelines apply:



Collaboration Server 1800 does not support

- ISDN connections
- · Video Switching Conferencing Mode
- A Recording Link that is being used by an ongoing conference cannot be deleted.
- A Recording Link that is assigned to a Profile cannot be deleted.
- The Recording Link supports H.264 High Profile with H.323 connections.
- While a Profile is being used in an ongoing conference, it cannot have a different Recording Link assigned to it.
- Up to 100 Recording Links can be listed for selection in the Conference Profile.
- Multiple Recording Links are supported in Continuous Presence and Video Switched conferences.
- The number of Recording Links available for selection is determined by the value of the MAXIMUM_RECORDING_LINKS System Flag in system.cfg. Default value is 20 Recording Links.

The recording link can be encrypted when recording from an encrypted conference to the RSS that
is set to encryption. For more details, see Recording Link Encryption.

Creating Multiple Virtual Recording Rooms on the RSS

If the environment includes a Polycom® RSS[™] 4000 Version 8.5 Recording and Streaming Server (RSS) and you want to associate Recording Links on the Collaboration Server with Virtual Recording Rooms (VRR), created and saved on the Polycom® RSS[™] 4000 Version 8.5 perform the following operations on the RSS:

- 1 Modify the parameters of a recording Template to meet the recording requirements.
- 2 Assign the modified recording Template to a VRR. The recording and streaming server will assign a number to the VRR.
- **3** Repeat step 1 and step 2 for each VRR to create additional VRRs. For more information see the RSS 4000 User Guide.

Configuring the Collaboration Server to Enable Recording

To make recording possible the following components you must be configured on the Collaboration Server:

- Recording Link Defines the connection between the conference and the recording system.
- Recording-enabled Conference IVR Service Recording DTMF codes and messages must be set in the Conference IVR Service to enable recording-related voice messages to be played and to allow the conference chairperson to control the recording process using DTMF codes.
- Recording-enabled Profile Recording must be enabled in the Conference Profile assigned to the recorded conference.

If Multiple Recording Links are being defined for Virtual Recording Rooms (VRRs), created and saved on the Polycom® RSS™ 4000 Version 8.5, the **MAXIMUM_RECORDING_LINKS** System Flag in **system.cfg** can be modified to determine the number of Recording Links available for selection.

Range: 20 - 100Default: 20

The flag value can be modified by selecting the *System Configuration* option from the *Setup* menu. For more information, see <u>Modifying System Flags</u>.

Defining the Recording Link

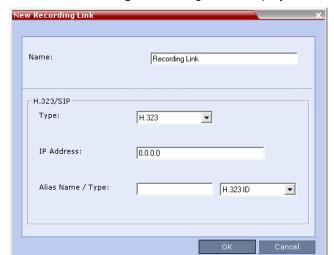
The Recording Link is defined once and can be updated when the H.323 alias or the IP address (of the recording system) is changed. Only one Recording Link can be defined in the Collaboration Server. Its type must be H.323.



In Multiple Networks Configuration, Recording Links use the default Network Service to connect to conferences, therefore the recording system must be defined on the default IP Network Service to enable the recording.

To define a Recording Link:

- 1 In the RMX Management pane, click Recording Links (
- 2 In the **Recording Links** list, click the **New Recording Link** (button.



The New Recording Link dialog box is displayed.

3 Define the following parameters:

Recording Link Parameters

Parameter	Description
Name	Displays the default name that is assigned to the Recording Link. If multiple Recording Links are defined, it is recommended to use a descriptive name to be indicate the VRR to which it will be associated. Default: Recording Link
Туре	Select the network environment: H.323 SIP
IP Address	 If no gatekeeper is configured, enter the IP Address of the RSS. Example: If the RSS IP address is 173.26.120.2 enter 173.26.120.2. If a gatekeeper is configured, you can either enter the IP address or an alias (see the alias description).

Parameter	Description
Alias Name	If using the endpoint's alias instead of IP address, first select the alias type and then enter the endpoint's alias.
	If you are associating this recording link to a VRR on the RSS, define the alias as follows:
	 If you are using the RSS IP address, enter the VRR number in the Alias field. For example, if the VRR number is 5555, enter 5555.
	 Alternatively, if the Alias Type is set to H.323 ID, enter the RSS IP address and the VRR number in the format:
	<rss_ip_address>##<vrr number=""></vrr></rss_ip_address>
	For example: If the RSS IP is 173.26.120.2 and the VRR number is 5555, enter 173.26.120.2##5555
Alias Type	Depending on the format used to enter the information in the IP address and Alias fields, select H.323 ID or E.164 (for multiple Recording links). E-mail ID and Participant Number are also available.

4 Click OK.

The Recording Link is added to the Collaboration Server unit.

Enabling the Recording Features in a Conference IVR Service

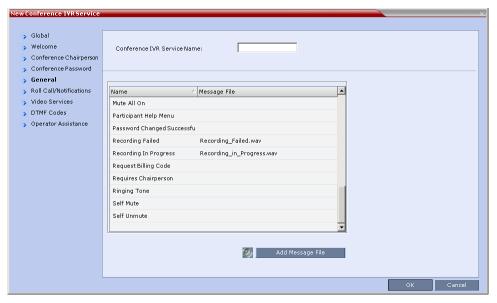
To record a conference, a Conference IVR Service in which the recording messages and DTMF codes are activated must be assigned to the conference. The default Conference IVR Service shipped with the Collaboration Server includes the recording-related voice messages and default DTMF codes that enable the conference chairperson to control the recording process from the endpoint. You can modify these default settings.

To modify the default recording settings for an existing Conference IVR Service:

- 1 In the RMX Management pane, click IVR Services (iii).
 - The IVR Services are listed in the IVR Services list pane.
- 2 To modify the default recording settings, double-click the Conference IVR Service or right-click and select **Properties**.

The Conference IVR Service Properties dialog box is displayed.

3 To assign voice messages other than the default, click the General tab and scroll down the list of messages to the recording messages.



- 4 Select the Recording In Progress message, and then select the appropriate message file (by default, Recording_in_Progress.wav) from the file list to the right of the field.
- 5 Select the Recording Failed message, and then select the appropriate message file (by default, Recording_Failed.wav) from the file list to the right of the field.
- 6 To modify the default DTMF codes, click the DTMF Codes tab.
- 7 To modify the DTMF code or permission for a recording function:
 - a Select the desired DTMF name (Start, Stop or Pause Recording), click the DTMF code entry and type a new code.

Default DTMF Codes assigned to the recording process

Recording Operation	DTMF Code	Permission
Start or Resume Recording	*3	Chairperson
Stop Recording	*2	Chairperson
Pause Recording	*1	Chairperson

- **b** In the **Permission** entry, select whether this function can be used by all conference participants or only the chairperson.
- 8 Click OK.

Enabling the Recording in the Conference Profile

To be able to record a conference, the recording options must be enabled in the Conference Profile assigned to it. You can add recording to existing Profiles by modifying them.

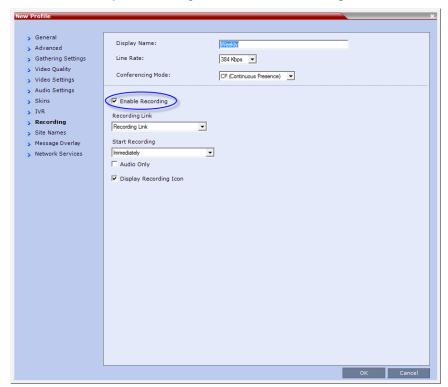
To enable recording for a conference:

- 1 In the Collaboration Server Management pane, click Conference Profiles (﴿).
 The Conference Profiles list is displayed.
- 2 Create a new profile by clicking **New Profile** (), or modify an existing profile by double-clicking or right-clicking an existing profile and then selecting **Profile Properties**.



If creating a new profile, complete the conference definition. For more information on creating Profiles see Defining AVC CP Conferencing Profiles.

3 In the **Profile Properties** dialog box, click the **Recording** tab.



- 4 Select the Enable Recording check box.
- 5 Define the following parameters

Conference Profile Recording Parameters:

Parameter	Description
Enable Recording	Select to enable Recording Settings in the dialog box.
Recording Link	Select a recording link for the conference from the list.

Parameter	Description
Start recording	 Select one of the following: Immediately – conference recording is automatically started upon connection of the first participant. Upon Request – the operator or chairperson must initiate the recording (manual).
Audio only	Select this option to record only the audio channel of the conference. Note: An Audio Only Recording Link cannot be used to record a conference if there are no Voice resources allocated in the Video/Voice Port Configuration.
Display Recording Icon	Select this option to display Recording Indication to all conference participants informing them that the conference is being recorded. The recording icon is replaced by a Paused icon when conference recording is paused.

6 Click OK.

Recording is enabled in the Conference Profile.

Recording Link Encryption

The Recording Link can be encrypted when recording an encrypted conference. The encryption of the Recording Link is enabled when Encryption is selected in the Conference Profile on the Collaboration Server and on the RSS, and the system flag

ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF is set to NO.

Recording Link Encryption Guidelines:

- The Recording Link connection type must be H.323.
- The Recording Link uses the AES encryption format.
- The RSS 4000 recorder must be set to support encryption. For more information see the RSS 4000 User Manual.
- Encryption must be selected in the Conference Profile.

Recording Link Encryption Flag Setting

Recording Links are treated as regular participants, however if the **ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF** System Flag is set to **YES** a non-encrypted Recording Link is to be allowed to connect to an encrypted conference.

The following table summarizes the connection possibilities for a Recording Link that is to be connected to a conference for each of the conference profile and Entry Queue encryption options.

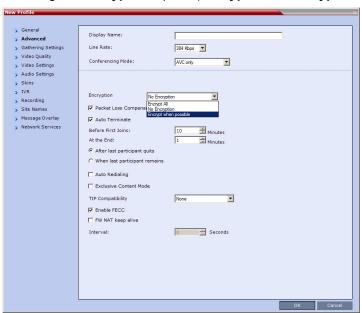
Connections by Recording Link and Conference Encryption Settings

Conference Profile	Recording Link Connection Status according to flag: ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_ CONF	
Setting	YES	NO
Encrypt All	Connected encrypted if possible, otherwise connected non-encrypted.	Connected only if encrypted, otherwise disconnected.
No Encryption	Connected non-encrypted.	Connected non-encrypted.
Encrypt when possible	Connected encrypted if possible, otherwise connected non-encrypted.	Connected encrypted if possible, otherwise connected non-encrypted.

Recording Link Settings

The recording of encrypted conferences via an encrypted Recording Link is enabled in the Conference Profile by:

Selecting the Encryption option (Encrypt All or Encrypt when Possible) in the Advanced tab.



For more details, see Packet Loss Compensation (LPR and DBA) AVC CP Conferences.

 Setting the Recording options in the Recording tab. For more details, see Enabling the Recording in the Conference Profile.

Managing the Recording Process

When a conference is started and recording is enabled in its Profile, the system will automatically start the recording if the Start Recording parameter is set to immediately. If it is set to Upon Request, the system waits for the chairperson or Collaboration Server user's request. Once the recording is initiated for a conference, the MCU connects to the recording device (RSS 2000/4000) using the default Recording Link. The connection that is created between the conference and the recording device is represented as a special participant (Recording) whose name is the Recording Link. Once the recording has started, the recording process can be stopped and restarted from the Chairperson's endpoint (using DTMF codes) or from the Collaboration Server Web Client. After the recording process has finished, the recording can be identified in the RSS 2000/4000 by its Collaboration Server conference name.



A conference participant and the Recording Link cannot have identical names, otherwise the recording process will fail.

Recording Link Layout

When the video layout of the conference is set to **Auto Layout**, the recording of the conference will now include all the conference participants and not n-1 participants as in previous versions.

In the new Auto Layout algorithm, the Recording Link is counted as a participant, and therefore it is excluded from the layout display used for the recording. The layout used for the other participants will behave as in the standard Auto Layout behavior.

The Recording Link Layout can be changed during an ongoing conference in the same manner as for any other conference participant. For more information see the Participant Level Monitoring.

The default settings for Auto Layout for the conference and the Recording Link are summarized in the following table:

Recording Link Default Layout Settings (Auto Layout Mode)

Participants	Conference Auto Layout Default Settings	Recording Link Auto Layout Settings
0	Not applicable	Not applicable
1		
2		
3		88
4		

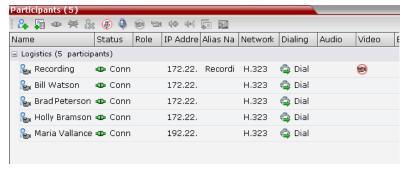
Participants	Conference Auto Layout Default Settings	Recording Link Auto Layout Settings
5		
6		
7		
8		
9		888
10 or more		0000 0000 0000

The default settings for Auto Layout of the Recording Link cannot be changed, and the Auto Layout flags do not apply to the Recording Link Auto Layout default settings.

Using the Collaboration Server Web Client to Manage the Recording Process

To manage the recording process using the right-click menu:

Right-click the Recording participant in the conference and select from one of the following options:



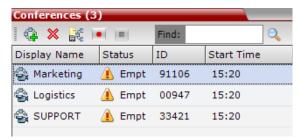
Recording Participant Right-click Options

Name	Description
Suspend Video	The Suspend Video option prevents the incoming video of the recording link participant to be part of the conference layout. The Recording Link participant is set by default to Suspend Video. The Suspend
	Video option toggles with the Resume Video option.

Name	Description
Resume Video	The Resume Video option enables the incoming video of the recording link participant to be part of the conference layout.
	This feature may be used to play back previously recorded video or audio feeds in the conference layout. For more information, see the RSS 4000 User Guide.
Participant Properties	The Participant Properties option displays viewing only information for monitoring, e.g. communication capabilities and channels used to connect to the conference. Users will not be able to perform any functional requests from this window, i.e. disconnect, change layout and mute.

To manage the recording process using the Conference toolbar:

In the Conferences pane, click one of the following buttons in the Conference tool bar.





The recording buttons will only be displayed in the conference tool bar for a conference that is recording-enabled.

Conferences List - Recording Tool bar buttons

Button	Description
•	Start/Resume recording. This button toggles with the Pause button.
	Stop recording.
Ш	Pause recording. This button toggles with the Start/Resume button.

Using DTMF Codes to Manage the Recording Process

By entering the appropriate DTMF code on the endpoint, the chairperson can **Stop** the recording (*74), **Pause** it (*75), or **Start/Resume** the recording (*73). For more information on managing the recording process via DTMF codes, see the *RSS 2000 User's Guide*.

Conference Recording with Codian IP VCR

Conference recording is available with Codian VCR 2210, VCR 2220 and VCR 2240.

Recording between the Collaboration Server and the Codian VCR is enabled by adding an IP participant to the recorded conference that acts as a link between the conference and the recording device. This participant is identified as a recording link to the Codian VCR according to the product ID sent from the VCR during the connection phase, in the call setup parameters.

The video channel between the conference and the recording device is unidirectional where the video stream is sent from the conference to the recorder.

If the Codian VCR opens a video channel to the conference - this channel is excluded from the conference video mix.

To record a conference running on the Collaboration Server using Codian recorder:

» In the conference, define or add a dial-out participant using the Codian VCR IP address as the address for dialing.

Once added to the conference, the MCU automatically connects the participant (the link to Codian VCR) and the recording is automatically started on the Codian VCR.

A connection can also be defined on the Codian VCR, dialing into the recorded conference using the MCU prefix and the Conference ID as for any other dial-in participant in the conference.

Monitoring the recording participant

This connection is monitored as any other participant in the conference. The connection can also be monitored in the Codian VCR web client.

Users, Connections, and Notes

Collaboration Server Users

Collaboration Server Web Client users are defined in the User's table and can connect to the MCU to perform various operations.

A maximum of 100 users can be defined per MCU.

User Types

The MCU supports the following user Authorization Levels:

- Administrator
- Operator
- Machine Account (Application-user)
- Administrator Read-only
- > Chairperson
- > Auditor



The following user types are not supported in Ultra Secure Mode:

- SUPPORT user
- Chairperson
- Auditor

Ultra Secure Mode is not supported with Collaboration Server 1800.

For more information see Ultra Secure Mode, User and Connection Management.



Users with **Auditor** authorization level cannot connect to the Collaboration Server via the RMX Manager application and must use the Collaboration Server Web Client.

The authorization level determines a user's capabilities within the system.

Administrator

An administrator can define and delete other users, and perform all configuration and maintenance tasks.

Administrator Read-only

A user with Administrator permission with the same viewing and monitoring permissions of a regular Administrator. However, this user is limited to creating system backups and cannot perform any other configuration or conference related operation.

Operator

An Operator can manage Meeting Rooms, Profiles, Entry Queues, and SIP Factories, and can also view the Collaboration Server configurations, but cannot change them.

Administrator and Operator users can verify which users are defined in the system. Neither of them can view the user passwords, but an Administrator can change a password.

Chairperson

A Chairperson can only manage ongoing conferences and participants. The Chairperson does not have access to the Collaboration Server configurations and utilities.

Auditor

An **Auditor** can only view Auditor Files and audit the system.

Machine Account

User names can be associated with servers (machines) to ensure that all users are subject to the same account and password policies. For more details, see Machine Account later on this chapter.

Listing Users

The **Users** pane lists the currently defined users in the system and their authorization levels. The pane also enables the administrators to add and delete users.

The system is shipped with a default Administrator user called POLYCOM, whose password is POLYCOM. However, once you have defined other authorized Administrator users, it is recommended to remove the default user.

You can view the list of users that are currently defined in the system.

To view the users currently defined in the system:

1 In the RMX Management pane, click Users ().

The **Users** pane is displayed.



The list includes three columns: User Name, Authorization Level and Disabled:

- > User Name The login name used by the user to connect to the MCU.
- > The Authorization Indicates the Authorization Level assigned to the User: Administrator, Administrator Read-only, Operator, Chairperson or Auditor.
- > **Disabled** Indicates whether the user is disabled and cannot access the system unless enabled by the administrator. For more details, see <u>Disabling a User</u>.

Locked indicates whether the user has been locked out and cannot access the system unless enabled by the administrator.

In Ultra Secure Mode (**ULTRA_SECURE_MODE=YES**), Users can be automatically disabled or locked out by the system when they do not log into the Collaboration Server application for a predefined period or if their login session does not meet Enhanced Security requirements. Users can be manually disabled by the administrator. For more details, see Notes.

Adding a New User

Administrators can add new users to the system.



The User Name and Password must be in ASCII.

To add a new user to the system:

- 1 In the RMX Management pane, click Users ().
- 2 The **Users** pane is displayed.

3 Click New User (), or right-click anywhere in the pane and then click New User.
The User Properties dialog box opens.



- 4 In the User Name text box, enter the name of the new user. This is the login name used by the user when logging into the system.
- 5 In the Password text box, enter the new user's password. This will be the user's password when logging into the system.
- 6 In the Authorization Level list, select the user type: Administrator, Administrator Read-Only, Operator, Chairperson or Auditor.
- 7 To associate a user with a machine:
 - a In the User Properties dialog box, select the Associate with a machine check box.
 - **b** Enter the FQDN of the server that hosts the application who's application-user name is being added. Example: cmal.polycom.com
- 8 Click OK.

The **User Properties** dialog box closes and the new user is added to the system.

Deleting a User



To delete a user, you must have Administrator authorization. The last remaining Administrator in the **Users** list cannot be deleted.

- 1 In the RMX Management pane, click Users ().
- 2 Select the user and click **Delete** (**>>**), or right-click the user and then click **Delete User**. The system displays a confirmation message.
- 3 In the **confirmation** dialog box, select **Yes** to confirm or **No** to cancel the operation. If you select **Yes**, the user name and icon are removed from the system.

Changing a User's Password

Users with Administrator authorization can change their own password and other users' passwords. Users with Operator authorization can change their own password.

To change a user's password:

- 1 In the RMX Management pane, click Users ().
- 2 Right-click the user and click Change User Password.

The Change Password dialog box opens.



3 Enter the Old Password (current), New Password and Confirm the New Password.



The Password must be in ASCII.

4 Click OK.

The user's password is changed.

Disabling a User

An administrator can disable an enabled user. An indication is displayed in the Users List when the User is disabled. An administrator can enable a disabled User.

To disable a user:

1 In the RMX Management pane, click Users ().

The Users pane is displayed.

2 In the Users pane, right-click the user to be disabled and select Disable User in the menu.



A confirmation box is displayed.



3 Click YES.

The User status in the Users list - Disabled column changes to Yes.

Enabling a User

An administrator can enable a User who was disabled automatically by the system (in the Ultra Secure Mode) or manually by the administrator.

To enable a user:

- 1 In the RMX Management pane, click Users (). The Users pane is displayed.
- 2 Right-click the user to be enabled and select **Enable User**.



A confirmation box is displayed.

3 Click YES.

The User status in the **Users** list - **Disabled** column changes to **NO**.

Renaming a User

To rename a user:

- 1 In the RMX Management pane, click Users (). The Users pane is displayed.
- 2 Right-click the user to be renamed and select **Rename User**.



The Rename User dialog box is displayed.



3 Enter the user's new name in the **New User Name** field and click **OK**.

The user is renamed and is forced to change his/her password.

Machine Account

User names can be associated with servers (machines) to ensure that all users are subject to the same account and password policies.

For enhanced security reasons it is necessary for the Collaboration Server to process user connection requests in the same manner, whether they be from regular users accessing the Collaboration Server via the Collaboration Server Web Browser / RMX Manager or from application-users representing applications such as CMA and RealPresence DMA system.

Regular users can connect from any workstation having a valid certificate while application-users representing applications can only connect from specific servers. This policy ensures that a regular user cannot impersonate an application-user to gain access to the Collaboration Server in order to initiate an attack that would result in a Denial of Service (DoS) to the impersonated application.

The connection process for an application-user connecting to the Collaboration Server is as follows:

- 1 The application-user sends a connection request, including its TLS certificate, to the Collaboration Server.
- **2** The Collaboration Server searches its records to find the FQDN that is associated with the application-user's name.
- **3** If the FQDN in the received certificate matches that associated with application-user, and the password is correct, the connection proceeds.

Guidelines for defining a machine account

- Application-users are only supported when TLS security is enabled and Request peer certificate is selected. TLS security cannot be disabled until all application-user accounts have been deleted from the system.
- For Secure Communications, an administrator must set up on the Collaboration Server system a
 machine account for the RealPresence CMA/DMA/XMA system with which it interacts. This machine
 account must include a fully-qualified domain name (FQDN) for the RealPresence CMA/DMA/XMA
 system.
- Application-user names are the same as regular user names.
 - **Example:** the CMA application could have an application-user name of CMA1.
- The FQDN can be used to associate all user types: Administrator, Operator with the FQDN of a server.
- Multiple application-users can be configured the same FQDN name if multiple applications are hosted on the same server
- If the system is downgraded the application-user's FQDN information is not deleted from the Collaboration Server's user records.
- A System Flag, PASS_EXP_DAYS_MACHINE, enables the administrator to change the password expiration period of application-user's independently of regular users. The default flag value is 365 days.
- The server hosting an application-user whose password is about to expire will receive a login response stating the number of days until the application-user's password expires. This is determined by the value of the PASSWORD_EXPIRATION_WARNING_DAYS System Flag. The earliest warning can be displayed 14 days before the password is due to expire and the latest warning can be displayed 7 days before passwords are due to expire. An Active Alarm is created stating the number of days before the password is due to expire.
- The MIN_PWD_CHANGE_FREQUENCY_IN_DAYS System Flag does not effect application-user accounts. Applications typically manage their own password change frequency.
- If an application-user identifies itself with an incorrect FQDN, its account will not be locked, however the event is written to the Auditor Event File.
- If an application-user identifies itself with a correct FQDN and an incorrect password, its account will be locked and the event written to the Auditor Event File.
- An application-user cannot be the last administrator in the system. The last administrator must be regular user.

User names are not case sensitive.

Monitoring

An application-user and its connection is represented by a specific icon.

Active Directory

- When working with Active Directory, CMA, RealPresence DMA system, and XMA cannot be registered within Active Directory as regular users. CMA and RealPresence DMA system application-users must be manually.
- The only restriction is that TLS mode is enabled together with client certificate validation.
- If the above configuration are set off it will not be possible to add machine accounts.
- When setting the TLS mode off the system should check the existence of a machine account and block this operation until all machine accounts are removed.

Connections

The Collaboration Server enables you to list all connections that are currently logged into the MCU, e.g. users, servers or API users. The MCU issues an ID number for each login. The ID numbers are reset whenever the MCU is reset.

A maximum of 50 users can be concurrently logged in to the MCU.

Viewing the Connections List

To list the users who are currently connected to the MCU:

1 In the Collaboration Server Management pane, click Connections (:::).

A list of connected users is displayed in the Connections pane.



The information includes:

- The user's login name.
- The user's authorization level (Chairperson, Operator, Administrator or Auditor).
- The time the user logged in.
- The name/identification of the computer used for the user's connection.

Notes

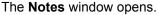
Notes are the electronic equivalent of paper sticky notes. You can use notes to write down questions, important phone numbers, names of contact persons, ideas, reminders, and anything you would write on note paper. Notes can be left open on the screen while you work.

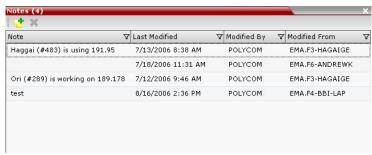
Notes can be read by all system Users concurrently connected to the MCU. Notes that are added to the Notes list are updated on all workstations by closing and re-opening the Notes window. Notes can be written in any Unicode language.

Using Notes

To create a note:

1 On the Collaboration Server menu, select Administration > Notes.

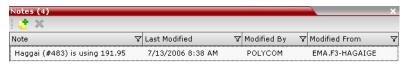




- 2 In the **Notes** toolbar, click **New Note** (), or right-click anywhere inside the **Notes** window and select **New Note**.
- 3 In the **Note** dialog box, type the required text and click **OK**.

The new note is saved and closed. The **Notes** list is updated, listing the new note and its properties:

- Note The beginning of the note's text.
- ➤ Last Modified The date of creation or last modification.
- > Modified By The Login Name of the user who last modified the note.
- Modified From The Client Application and Workstation from which the note was created or modified.



To open or edit a note:

» Double-click the entry to edit, or right-click the entry and select **Note Properties**.
The note opens for viewing or editing.

To delete a note:

- 1 In the **Notes** list, select the entry for the note to delete and click **Delete Note** (**≥**), or right-click the entry and select **Delete Note**.
 - A **delete confirmation** dialog box is displayed.
- 2 Click **OK** to delete the note, or click **Cancel** to keep the note.

IP Network Services

IP Network Services enable the RealPresence Collaboration Server to function within IP network environments. They include the network parameters required for the MCU to connect with other IP devices on the same network or outside the network through a firewall.

Collaboration Server IP Network Services Overview

Two types of IP Network Services are defined for the Collaboration Server:

- Management Network Service
- Default IP Service (Conferencing Service)

Connection between the Collaboration Server management applications (Web Client And RMX Manager) and participant connections to conferences (Dial in, dial out) are supported within the following IP addressing environments: IPv4, IPv6 and IPv6 & IPv4

When IPv4 is selected, IPv6 fields are hidden and conversely when IPv6 is selected, IPv4 fields are hidden. When IPv6 & IPv4 is selected both IPv6 and IPv4 fields are displayed.

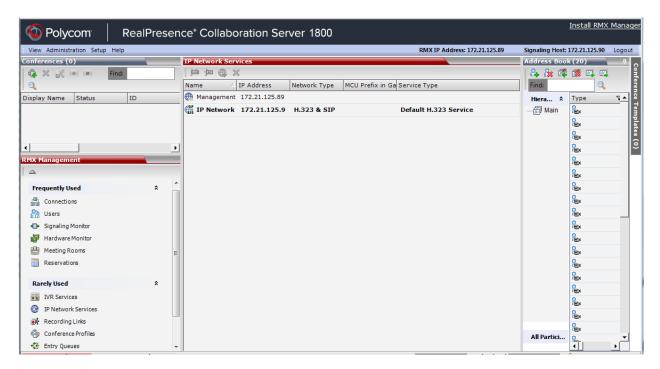


For the purposes of comprehensive documentation, all screen captures in this chapter pertaining to Collaboration Servers (RMX) 1500/1800/2000/4000 show the dialog boxes as displayed with IPv6 & IPv4 selected.

For more information on IPv6, see LAN Redundancy.

When the RMX is configured for IPv4 and IPv6 Addressing, the addition of the **sdp-anat** option tag in the SIP Require and SIP Supported headers allows a mixture of IPv4 and IPv6 addressing to be specified by the Session Description Protocol (SDP). For more information see Management Network (Primary).

The **IP Network Services** are configured by selecting this option in the **RMX Management** pane of the Collaboration Server Web Client/RMX Manager application.



Management Network (Primary)

The Management Network is used to connect between the Collaboration Server and the management applications (Collaboration Server Web Client or RMX Manager application) and enable these applications to control the MCU. It contains the network parameters, such as the IP address of the MCU's control unit, required for connection between the Collaboration Server and the management applications. You can use this IP address to connect to the control unit should the MCU become corrupted or inaccessible.

During First Time Power-up, the Management Network parameters can be set either via a USB key or by using a cable to create a private network. For more information, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, First Entry Power-up and Configuration and Appendix G - Configuring Direct Connections to the Collaboration Server.

Default IP Service (Conferencing Service)

The Default IP Service (Conferencing Service) is used to configure and manage communications between the Collaboration Server and conferencing devices such as endpoints, gatekeepers, SIP servers, etc.

The Default IP Service contains parameters for:

- Signaling Host IP Address
- External conferencing devices

Calls from all external IP entities are made to the Signaling Host, which initiates call set-up and assigns the call to the appropriate media card.

Conferencing related definitions such as environment (H.323 or SIP) are also defined in this service.

Most of the Default IP Service is configured by the **Fast Configuration Wizard**, which runs automatically should the following occur:

- First time power-up.
- Deletion of the Default IP Service, followed by a system reset.

For more information, see the *Polycom® RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, First Entry Power-up and Configuration



Changes made to any of these parameters only take effect when the Collaboration Server is reset. An Active Alarm is created when changes made to the system have not yet been implemented and the MCU must be reset.

Using IPv6 Networking Addresses for Collaboration Server Internal and External Entities

IPv6 addresses can be assigned to both Collaboration Server (Internal) and External Entity addresses.

Collaboration Server Internal Addresses (Default Management Network Service):

- Control Unit
- Signaling Host
- Shelf Management
- MPM1 (Media Card)
- MPM2 (Media Card)

External Entities:

- Gatekeepers (Primary & Secondary)
- SIP Proxies on EMA
- DNS Servers
- Default Router
- Defined participants

IPv6 Addressing Guidelines

- Internet Explorer 7™ is required for the Collaboration Server Web Client and RMX Manager to connect to the Collaboration Server using IPv6.
- The default IP address version is IPv4.
- The IP address field in the Address Book entry for a defined participant can be either IPv4 or IPv6. A
 participant with an IPv4 address cannot be added to an ongoing conference while the Collaboration
 Server is in IPv6 mode nor can a participant with an IPv6 address be added while the Collaboration
 Server is in IPv4 mode.
 - An error message, Bad IP address version, is displayed and the New Participant dialog box remains open so that the participant's address can be entered in the correct format.
- Participants that do not use the same IP address version as the Collaboration Server in ongoing conferences launched from Meeting Rooms, Reservations and Conference Templates, and are disconnected. An error message, Bad IP address version, is displayed.
- IP Security Protocols (IPSec) are not supported.

Modifying the Management Network

The Management Network parameters need to be modified if you want to:

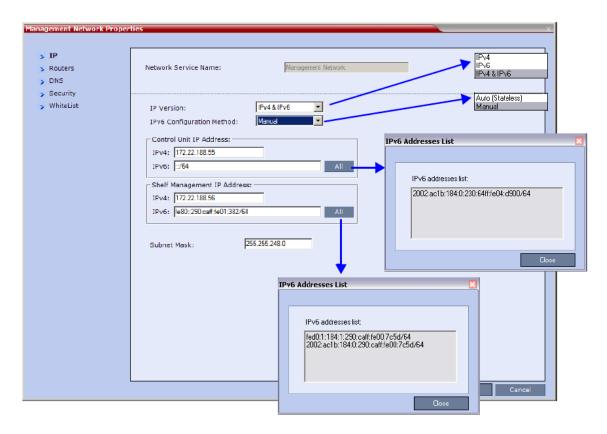
- Connect directly to the Collaboration Server from a workstation
- Modify routes
- Modify DNS information

To view or modify the Management Network Service:

- 1 In the RMX Management pane, click the IP Network Services () button.
- 2 In the IP Network Services list pane, double-click the Management Network () entry.

 The Management Network Properties IP dialog box opens

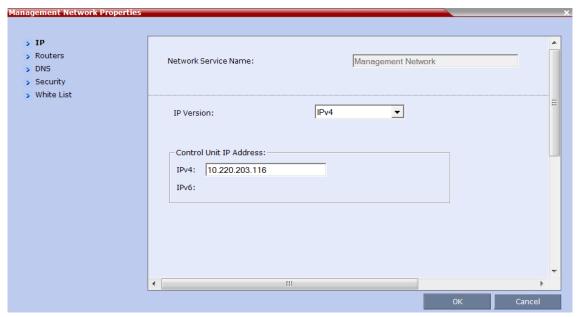
Management Network Properties - Collaboration Servers (RMX) 1500/2000/4000





On the RealPresence Collaboration Server (RMX) 2000 an additional tab called ${\bf LAN~Ports}$ appears. For more information on the ${\bf LAN~Ports}$ tab see Step 8.

Management Network Properties - Collaboration Server (RMX) 1800



3 Modify the following fields:

Default Management Network Service - IP

Field	Description	
Network Service Name	Displays the name of the Management Network. This name cannot be modified. Note: This field is displayed in all Management Network Properties tabs.	
IP Version	IPv4	Select this option for IPv4 addressing only.
	IPv6	Select this option for IPv6 addressing only.
	IPv4 & IPv6	Select this option for both IPv4 and IPv6 addressing. Note: If the gatekeeper cannot operate in IPv6 addressing mode, the H323_RAS_IPV6 System Flag should be set to NO. For more information see Manually Adding Flags to the CS_MODULE_PARAMETERS Tab.

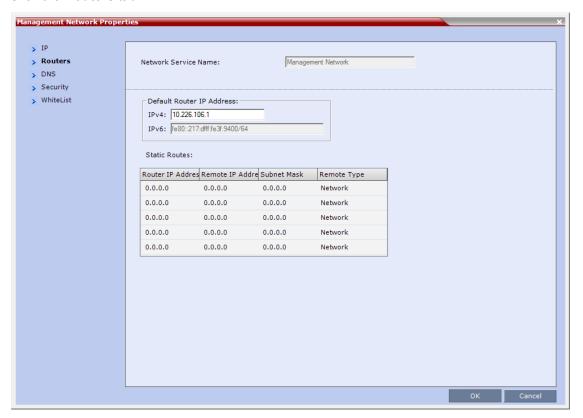
Default Management Network Service - IP

Field	Description	
IPv6 Configuration Method Manual Configuration Method is recommended with IPv6.	Auto (Stateless)	Select this option to allow automatic generation of the following addresses: Link-Local (For internal use only) Site-Local Global
	Manual	Select this option to enable manual entry of the following addresses: Site-Local Global Manual configuration of the following address types is not permitted: Link-Local Multicast Anycast
Control Unit IP Address	IPv4	The IPv4 address of the Collaboration Server. This IP address is used by the Collaboration Server Web Client to connect to the Collaboration Server.
	IPv6	The IPv6 address of the MCU. This IP address is used by the Collaboration Server Web Client to connect to the Collaboration Server. Note: Internet Explorer 7™ is required for the Collaboration Server Web Client to connect to the MCU using IPv6. All Click the All button to display the IPv6 addresses as follows: • Auto - If selected, Site-Local and Global site addresses are displayed. • Manual - If selected, only the Manual site address is displayed.

Default Management Network Service - IP

Field	Description	
Shelf Management IP Address Collaboration Server 1500/2000/4000 only)	IPv4	The IPv4 address of the RMX Shelf Management Server. This IP address is used by the Collaboration Server Web Client for Hardware Monitoring purposes.
	IPv6	The IPv6 address of the RMX Shelf Management Server. This IP address is used by the Collaboration Server Web Client for Hardware Monitoring purposes. Note: Internet Explorer 7™ is required for the Collaboration Server Web Client to connect to the MCU using IPv6.
		All Click the All button to display the IPv6 addresses as follows: • Auto - If selected, Site-Local and Global site addresses are displayed. • Manual - If selected, only the Manual site address is displayed.
Subnet Mask	Enter the subnet mask on Note: This field is specification.	of the Control Unit. Fic to IPv4 and is not displayed in IPv6 only mode.

4 Click the Routers tab.

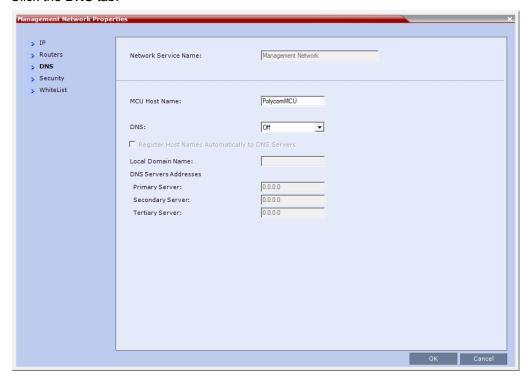


5 Modify the following fields:

Default Management Network Service – Routers

Field	Description	
Default Router IP Address	IPv4	Enter the IP address of the default router. The default router
	IPv6	is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.
Static Routes (IPv4 Only Table)		The system uses Static Routes to search other networks for endpoint addresses that are not found on the local LAN. Up to five routers can be defined in addition to the Default Router. The order in which the routers appear in the list determines the order in which the system looks for the endpoints on the various networks. If the address is in the local subnet, no router is used. To define a static route (starting with the first), click the appropriate column and enter the required value.
	Router IP Address	Enter the IP address of the router.
	Remote IP Address	 Enter the IP address of the entity to be reached outside the local network. The Remote Type determines whether this entity is a specific component (Host) or a network. If Host is selected in the Remote Type field, enter the IP address of the endpoint. If Network is selected in the Remote Type field, enter of the segment of the other network.
	Remote Subnet Mask	Enter the subnet mask of the remote network.
	Remote Type	Select the type of router connection:
		Network – defines a connection to a router segment in another network.
		Host – defines a direct connection to an endpoint found on another network.

6 Click the DNS tab.

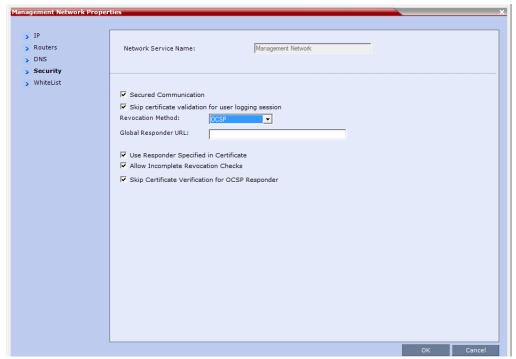


7 Modify the following fields:

Default Management Network Service - DNS

Field	Description
MCU Host Name	Enter the name of the MCU on the network. Default name is RMX
DNS	Select: Off – If DNS servers are not used in the network. Specify –To enter the IP addresses of the DNS servers. Note: The IP address fields are enabled only if Specify is selected.
Register Host Names Automatically to DNS Servers	Select this option to automatically register the MCU Signaling Host and Shelf Management with the DNS server.
Local Domain Name	Enter the name of the domain where the MCU is installed.
DNS Servers Addresses:	
Primary Server	The static IP addresses of the DNS servers.
Secondary Server	A maximum of three servers can be defined.
Tertiary Server	

8 Click the Security tab.



9 Modify the following fields:

Management Network Properties – Security Parameters

Field	Description
Secured Communication	Select to enable Secured Communication. The Collaboration Server supports TLS 1.0 and SSL 3.0 (Secure Socket Layer). A SSL/TLS Certificate must installed on the Collaboration Server for this feature to be enabled. For more information see Appendix F- Secure Communication Mode.
Skip certificate validation for user logging session	Select this check box to prevent peer certificate requests being issued. For more information see (PKI) Public Key Infrastructure. This check box must be cleared when enabling Secured Mode. If it is not cleared an Active Alarm is created and a message is displayed stating that Secured Communications Mode must be enabled.
Revocation Method	
Global Responder URL	For a detailed description of these fields see Certificate Managementand Certificate Revocation.
Use Responder Specified in Certificate	Note: Ultra Secure Mode and these options are not supported with Collaboration Server 1800.
Allow Incomplete Revocation Checks	

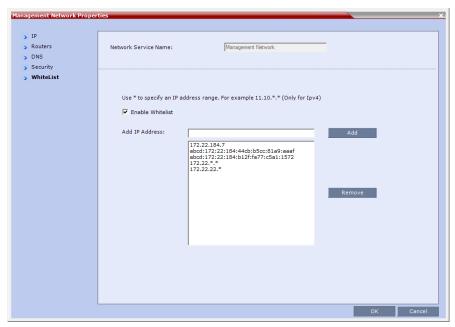
Management Network Properties - Security Parameters

Field	Description
Skip Certificate Validation for OSCP Responder	For a detailed description see Certificate Management and Certificate Revocation. Note: Ultra Secure Mode and these options are not supported with Collaboration Server 1800.

10 Click OK.

- 11 If you have modified the Management Network Properties, reset the MCU.
- **12** To define a white list, click the **Whitelist** tab. (For Collaboration Servers (RMX) 1500/1800/2000/4000 only.)

A **White List** contains the addresses of IP Networking Entities permitted to connect to the RMX's Management Network; Networking Entities such as Network Hosts, Control Workstations, Gatekeepers SIP/ DNS Servers, etc.



For a detailed description of these fields see White List Access.

Modifying the Default IP Network Service

The Default IP Network Service is defined initially during the First Time Power-up or if the Default IP Service has been deleted, followed by an Collaboration Server restart. For details, see *Polycom® RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Procedure 4: Modifying the Default IP Service and ISDN/PSTN Network Service Settings.

Once the Default IP Network Service is defined, you can modify its properties through the IP Network Properties dialog boxes. The Default IP Service parameters need to be modified if you want to change the:

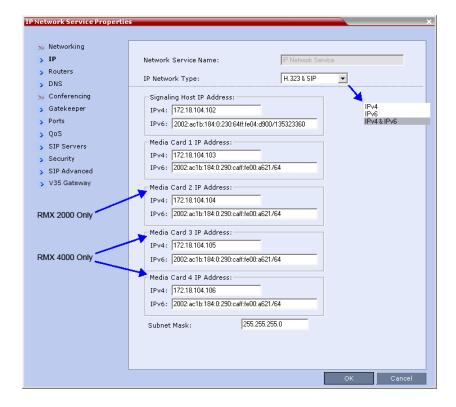
- Network type that the Collaboration Server connects to
- IP address of the Collaboration Server Signaling Host
- IP addresses of the Collaboration Server Media boards
- Subnet mask of the Collaboration Server's IP cards
- Gatekeeper parameters or add gatekeepers to the Alternate Gatekeepers list
- SIP server parameters

To view or modify the Default IP Service:

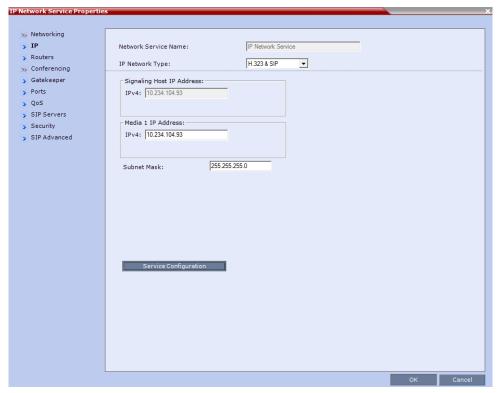
- 1 In the RMX Management pane, click IP Network Services ().
- 2 In the Network list pane, double-click the Default IP Service (, , , or) entry.

The **Default IP Service - Networking IP** dialog box is displayed.

Default IP Service - Collaboration Servers (RMX) 1500/2000/4000







3 Modify the following fields:

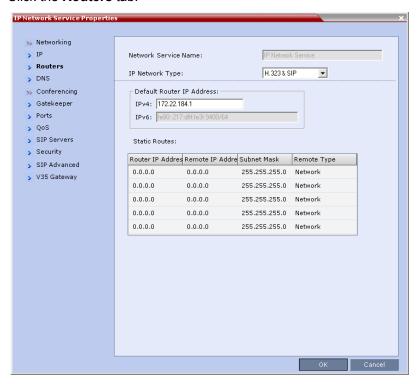
Default IP Network Service - IP

Field	Description	
Network Service Name	The name Default IP Service is assigned to the IP Network Service by the Fast Configuration Wizard. This name can be changed. Note: This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.	
IP Network Type	Displays the network type selected during the First Entry configuration. The Default IP Network icon indicates the selected environment. You can select: H.323 - For an H.323-only Network Service. SIP - For a SIP-only Network Service. H.323 & SIP - For an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this service. Note: This field is displayed in all Default IP Service tabs.	

Default IP Network Service - IP

Field	Description	
Signaling Host IP Address	On RealPresence Collaboration Server 1800 this field is disabled as only one IP address is used for signaling and media transmission. Enter the address to be used by IP endpoints when dialing in to the MCU. Dial out calls from the Collaboration Server are initiated from this address. This address is used to register the Collaboration Server with a Gatekeeper or a SIP Proxy server.	
Media Card 1 IP Address	Collaboration Server 1500/1800: Enter the IP address of the media card to be used by IP endpoints when dialing in to the MCU. Collaboration Server 200/4000: Enter the IP address of the first media card as provided by the network administrator.first media card Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.	
Media Card 2 IP Address (Collaboration Server 2000/4000)	Collaboration Server 2000/4000: Enter the IP address of the second media card if installed. Endpoints connect to conferences and transmit call media (video, voice and content) via these address.	
Media Card 3 IP Address (Collaboration Server 4000)	Collaboration Server 4000: Enter the IP address of the third media cards if installed. Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.	
Media Card 4 IP Address (Collaboration Server 4000)	Collaboration Server 4000: Enter the IP address of the fourth media cards if installed. Endpoints connect to conferences and transmit call media (video, voice and content) via these addresses.	
Subnet Mask	Enter the subnet mask of the MCU. Default value: 255.255.255.0.	

4 Click the Routers tab.

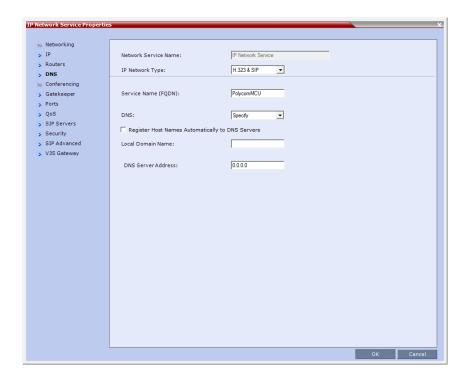


With the exception of **IP Network Type**, the field definitions of the **Routers** dialog box are the same as for the Default Management Network. For more information see Default Management Network Service – Routers.

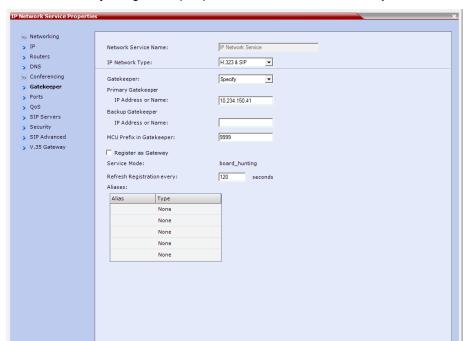
5 Optional. Click the DNS tab.



DNS configuration is not applicable to the RealPresence Collaboration Server (RMX) 1800.



- 6 In the DNS field select Specify.
- 7 In the DNS Server Address field, enter the IP address of the DNS Server for the IP Network Service.
 - ➤ If the DNS field in the IP Network Service is set to **Specify** and the DNS is not configured or disabled, the DNS configured for the Management Network will be used.
 - When upgrading from a version that does not support a DNS per IP Network Service, the DNS configured for the Management Network will be used.
 - In both Standard Security and Ultra Secure Modes:
 - A separate DNS can be configured for the Management Network Service and the IP Network Service.
 - ◆ If a Multiple Services Licence is installed, a separate DNS can be configured for each additional IP Network Service that is defined. For more information see Multiple Network Services.



8 To view or modify the gatekeeper parameters, click the **Gatekeeper** tab.

9 Modify the following fields:

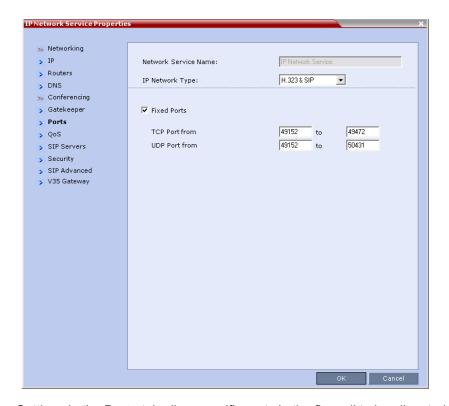
Default IP Service - Conferencing - Gatekeeper Parameters

Field	Description	
Gatekeeper	Select Specify to enable configuration of the gatekeeper IP address. When Off is selected, all gatekeeper options are disabled.	
Primary Gatekeeper IP Address or Name	Enter either the gatekeeper's host name as registered in the DNS or IP address.	Note: When in IPv4&IPv6 or in
Alternate Gatekeeper IP Address or Name	Enter the DNS host name or IP address of the gatekeeper used as a fallback gatekeeper used when the primary gatekeeper is not functioning properly.	 IPv6 mode, it is easier to use Names instead of IP Addresses.
MCU Prefix in Gatekeeper	Enter the number with which this Network Service registers in the gatekeeper. This number is used by H.323 endpoints as the first part of their dial-in string when dialing the MCU. When PathNavigator or SE200 is used, this prefix automatically registers with the gatekeeper. When another gatekeeper is used, this prefix must also be defined in the gatekeeper.	
Register as Gateway	Select this check box if the Collaboration Server is to be seen as a gateway, for example, when using a Cisco gatekeeper. Note: Do not select this check box when using Polycom ReadiManager/CMA 5000 or a Radvision gatekeeper.	

Default IP Service – Conferencing – Gatekeeper Parameters

Field	Description	
Refresh Registration every seconds	The frequency with which the system informs the gatekeeper that it is active by re-sending the IP address and aliases of the IP cards to the gatekeeper. If the IP card does not register within the defined time interval, the gatekeeper will not refer calls to this IP card until it re-registers. If set to 0, re-registration is disabled. Note: It is recommended to use default settings.	
	 This is a re-registration and not a 'keep alive' operation – an alternate gatekeeper address may be returned. 	
Aliases		
Alias	The alias that identifies the Collaboration Server's Signaling Host within the network. Up to five aliases can be defined for each Collaboration Server. Note: When a gatekeeper is specified, at least one alias must be entered in the table. Additional aliases or prefixes may also be entered.	
Туре	The type defines the format in which the card's alias is sent to the gatekeeper. Each alias can be of a different type: H.323 ID (alphanumeric ID) E.164 (digits 0-9) Email ID (email address format, e.g. abc@example.com) Participant Number (digits 0-9, * and #) Note: Although all types are supported, the type of alias to be used depends on the gatekeeper's capabilities.	

¹⁰ To view or modify the ports values, click the **Ports** tab.



Settings in the **Ports** tab allow specific ports in the firewall to be allocated to multimedia conference calls.

The port range recommended by IANA (Internet Assigned Numbers Authority) is 49152 to 65535. The Collaboration Server uses this recommendation along with the number of licensed ports to calculate the port range.

11 Modify the following fields:

Default IP Service – Conferencing – Ports Parameters

Field	Description
Fixed Ports	Leave this check box cleared if you are defining a Network Service for local calls that do not require configuring the firewall to accept calls from external entities. When cleared, the system uses the default port range and allocates 4 RTP and 4 RTCP ports for media channels (Audio, Video, Content and FECC).
	Note: When ICE Environment is enabled, 8 additional ports are allocated to each call.
	Click this check box to manually define the port ranges or to limit the number of ports to be left open.
TCP Port from - to	Displays the default settings for port numbers used for signaling and control.
	To modify the number of TCP ports, enter the first and last port numbers in the range.
	The number of ports is calculated as follows:
	Number of simultaneous calls x 2 ports (1 signaling + 1 control).

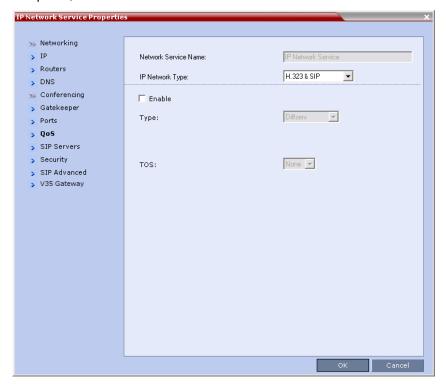
Default IP Service - Conferencing - Ports Parameters

Field	Description
UDP Port from - to	Displays the default settings for port numbers used for audio and video. To modify the number of UDP ports: Enter the first and last port numbers in the range, and the range must be 1024 ports per media card. When ICE environment is enabled, the range must be 2048 ports per media card.



If you do not specify an adequate port range, the system will accept the settings but will issue a warning. Calls will be rejected when the Collaboration Server's ports are exceeded.

12 If required, click the QoS tab.



Quality of Service (QoS) is important when transmitting high bandwidth audio and video information. QoS can be measured and guaranteed in terms of:

- · Average delay between packets
- Variation in delay (jitter)
- · Transmission error rate

DiffServ and **Precedence** are the two QoS methods supported by the Collaboration Server. These methods differ in the way the packet's priority is encoded in the packet header.

The Collaboration Server's implementation of QoS is defined per Network Service, not per endpoint.



The routers must support QoS in order for IP packets to get higher priority.

13 View or modify the following fields:

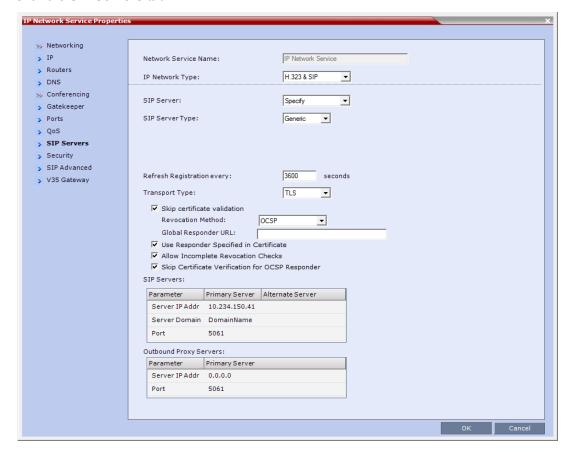
Default IP Service - Conferencing - QoS Parameters

Field	Description
Enable	Select to enable the configuration and use of the QoS settings. When un-checked, the values of the DSCP (Differentiated Services Code Point) bits in the IP packet headers are zero.
Туре	 DiffServ and Precedence are two methods for encoding packet priority. The priority set here for audio video and IP Signaling packets should match the priority set in the router. DiffServ: Select when the network router uses DiffServ for priority encoding. The default priorities for both audio and video packets is 0x31. These values are determined by the QOS_IP_VIDEO and QOS_IP_AUDIO flags in the system.cfg file. The default priority for Signaling IP traffic is 0x00 and is determined by the QOS_IP_SIGNALING flag in the system.cfg file. For more information Modifying System Flags. Precedence: Select when the network router uses Precedence for priority encoding, or when you are not sure which method is used by the router. Precedence should be combined with None in the TOS field. The default priority is 5 for audio and 4 for video packets. Note: Precedence is the default mode as it is capable of providing priority services to all types of routers, as well as being currently the most common mechanism.
Audio / Video	You can prioritize audio and video IP packets to ensure that all participants in the conference hear and see each other clearly. Select the desired priority. The scale is from 0 to 5, where 0 is the lowest priority and 5 is the highest. The recommended priority is 4 for audio and 4 for video to ensure that the delay for both packet types is the same and that audio and video packets are synchronized and to ensure lip sync.

Default IP Service - Conferencing - QoS Parameters

TOS Select the type of Service (TOS) that defines optimization tagging for routing the conferences audio and video packets. • Delay: The recommended default for video conferencing; prioritized audio and video packets tagged with this definition are delivered with minimal delay (the throughput of IP packets minimizes the queue sequence and the delay between packets). • None: No optimization definition is applied. This is a compatibility mode in which routing is based on Precedence priority settings only. Select None if you do not know which standard your router supports.

14 Click the SIP Servers tab.



15 Modify the following fields:

Default IP Network Service - SIP Servers

Field	Description	
SIP Server	Select: • Specify – To manually configure SIP servers. • Off – If SIP servers are not present in the network. Note: When set to Specify, the Security tab is displayed.	
SIP Server Type	Select: • Generic - For non Microsoft environments. • Microsoft - For Microsoft SIP environments.	
Refresh Registration	This defines the time in seconds, in which the Collaboration Server refreshes it's registration on the SIP server. For example, if "3600" is entered the Collaboration Server will refresh it's registration on the SIP server every 3600 seconds.	
Transport Type	Select the protocol that is used for signaling between the Collaboration Server and the SIP Server or the endpoints according to the protocol supported by the SIP Server: UDP – Select this option to use UDP for signaling. TCP – Select this option to use TCP for signaling. TLS – The Signaling Host listens on secured port 5061 only and all outgoing connections are established on secured connections. Calls from SIP clients or servers to non secured ports are rejected. The following protocols are supported: TLS 1.0, SSL 2.0 and SSL 3.0. Note: If TLS is selected, the Skip Certificate Validation and the other certificate related fields are displayed.	
Skip Certificate Validation	When checked, no Certificate Validation is performed.	
Revocation Method		
Global Responder URL		
Use Responder Specified in Certificate	For a detailed description, see Certificate Managementand Certificate Revocation.	
Allow Incomplete Revocation Checks	Note: Ultra Secure Mode and these options are not supported with Collaboration Server 1800.	
Skip Certificate Validation for OSCP Responder		
SIP Servers: Primary / Alternate Server Parameter		
Server IP Address	Enter the IP address of the preferred SIP server. If a DNS is used, you can enter the SIP server name. Note: When in IPv4&IPv6 or in IPv6 mode, it is easier to use Names instead of IP Addresses.	

Default IP Network Service - SIP Servers

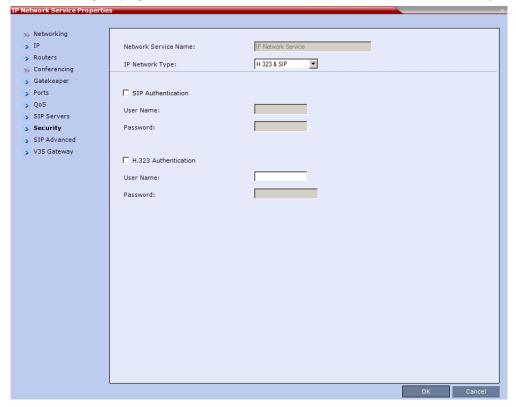
Field	Description	
Server Domain Name	Enter the name of the domain that you are using for conferences, for example: user_name@domain name	
	The domain name is used for identifying the SIP server in the appropriate domain according to the host part in the dialed string.	
	For example, when a call to EQ1@polycom.com reaches its outbound proxy, this proxy looks for the SIP server in the polycom.com domain, to which it will forward the call.	
	When this call arrives at the SIP server in polycom.com, the server looks for the registered user (EQ1) and forwards the call to this Entry Queue or conference.	
Port	Enter the number of the TCP or UDP port used for listening. The port number must match the port number configured in the SIP server. Default port is 5060.	
Outbound Proxy Servers: Primary / Alternate Server Parameter		
Server IP Address	By default, the Outbound Proxy Server is the same as the SIP Server. If they differ, modify the IP address of the Outbound Proxy and the listening port number (if required).	
	Note: When in IPv4&IPv6 or in IPv6 mode, it is easier to use Names instead of IP Addresses.	
Port	Enter the port number the outbound proxy is listening to. The default port is 5060.	



When updating the parameters of the SIP Server in the **IP Network Service - SIP Servers** dialog box, the Collaboration Server must be reset to implement the change.

16 Click the **Security** tab.

(This tab is only displayed if the SIP Server field in the SIP Servers tab is set to Specify.)



17 Modify the following fields:

Default IP Network Service - Security (SIP Digest)

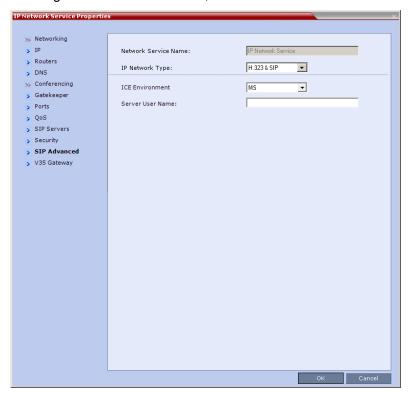
Field	Description	
SIP Authentication	Click this check box to enable SIP proxy authentication. Select this check box only if the authentication is enabled on the SIP proxy, to enable the Collaboration Server to register with the SIP proxy. If the authentication is enabled on the SIP proxy and disabled on the RMX, calls will fail to connect to the conferences. Leave this check box cleared if the authentication option is disabled on the SIP proxy.	
User Name	Enter the user name the Collaboration Server will use to authenticate itself with the SIP proxy. This name must be defined in the SIP Proxy.	These fields can contain up to 20 ASCII characters.
Password	Enter the password the Collaboration Server will use to authenticate itself with the SIP proxy. This password must be defined in the SIP proxy.	-

Default IP Network Service - Security (SIP Digest)

Field	Description	
H.323 Authentication	Click this check box to enable H.323 server authentication. Select this check box only if the authentication is enabled on the gatekeeper, to enable the Collaboration Server to register with the gatekeeper. If the authentication is enabled on the gatekeeper and disabled on the RMX, calls will fail to connect to the conferences. Leave this check box cleared if the authentication option is disabled on the gatekeeper.	
User Name	Enter the user name the Collaboration Server will use to authenticate itself with the gatekeeper. This name must be defined in the gatekeeper.	These fields can contain up to 64 ASCII characters.
Password	Enter the password the Collaboration Server will use to authenticate itself with the gatekeeper. This password must be defined in the gatekeeper.	_

If the **Authentication User Name** and **Authentication Password** fields are left empty, the SIP Digest authentication request is rejected. For registration without authentication, the Collaboration Server must be registered as a trusted entity on the SIP server.

18 To configure the ICE environment, click the SIP Advanced tab.



19 Modify the following fields:

Default IP Network Service - SIP Advanced

Field	Description
ICE Environment	Select MS (for Microsoft ICE implementation) to enable the ICE integration.
Server User Name	Enter the <i>Collaboration Server</i> User name as defined in the Active Directory . For example, enter rmx1234 . This field is disabled if the ICE Environment field is set to None .

20 To view or modify the V35 gateway parameters, click the V35 Gateway tab.



Serial Gateways are not supported on the RealPresence Collaboration Server (RMX) 1800.

The **V35 Gateway** dialog box is displayed.



21 Modify the following fields:

Network Service - V35 tab

Field	Description
V35 Gateway IP Address	Enter the Management IP address of the management interface of the Serial Gateway . For more information see the <i>RealPresence Collaboration Server</i> (<i>RMX</i>) 1500/2000/4000 Deployment Guide for Maximum Security Environments, Deploying a Polycom RMX [™] Serial Gateway S4GW.
Username	Enter the User Name that the Collaboration Server uses to log in to the management interface of the Serial Gateway.

Network Service - V35 tab

Field	Description
Password	Enter the Password that the Collaboration Server uses to log in to management interface of the Serial Gateway .

22 Click the OK button.



When updating the parameters of the SIP Server in the **IP Network Service - SIP Servers** dialog box, the Collaboration Server must be reset to implement the change.

Ethernet Settings

The automatically identified speed and transmit/receive mode of each **LAN** port used by the system can be manually modified if a specific switch requires it. These settings can be modified in the **Ethernet Settings** dialog box.



RealPresence Collaboration Server (RMX) 1500: The Port numbers displayed in the dialog box do not reflect the physical Port numbers as labeled on the RealPresence Collaboration Server (RMX) 1500.

The following table lists the physical mapping of Port Type to the physical label on the back panel of the RealPresence Collaboration Server (RMX) 1500.

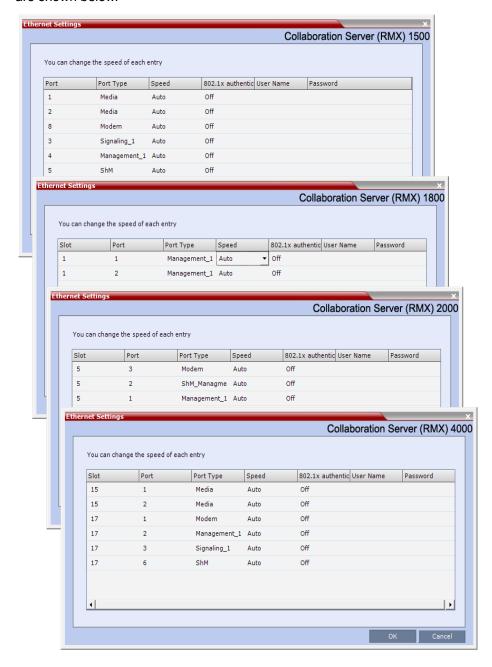
Physical Mapping - Port Type to Label on RealPresence Collaboration Server 1500/4000

Port Type		Label on MCU		
	1500	4000		
Media	LAN 2	LAN 2	RTM LAN Card	
Modem	Modem	LAN 1		
Management 1	MNG B	LAN 2	RTM-IP 4000 Card	
Signaling 1	MNG	LAN 3	KTW-IF 4000 Calu	
ShM	Shelf	LAN 6		

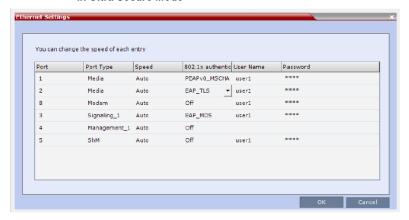
To modify the automatic LAN port configuration:

1 On the Collaboration Server menu, select **Setup > Ethernet Settings**.

The **Ethernet Settings** dialog box specific to the system you are using is displayed; some examples are shown below.



RealPresence Collaboration Server (RMX) 4000 in Ultra Secure Mode

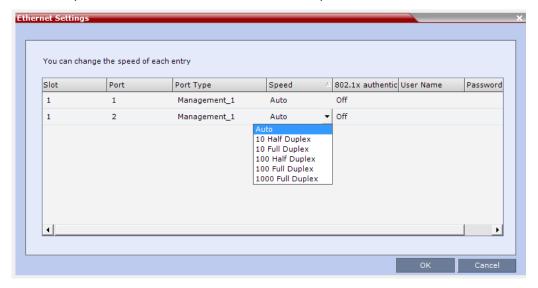




RealPresence Collaboration Server (RMX) 1500/4000 :

Although the RTM LAN (media card) ports are shown as Port 1 in the **Ethernet Settings** and **Hardware Monitor**, the physical LAN connection is **Port 2**.

2 Select the speed and transmit/receive mode for each ports as follows:



Ethernet Settings Parameters

Field	Description		
Speed	The Collaboration Server 1500/1800 has 2 LAN ports that can be configured. The Collaboration Server 2000/4000 has 3 LAN ports on the RTM-IP (Management, Signaling and Shelf Management), and additional LAN ports on each media card (RTM LAN) and RTM ISDN cards. You can set the speed and transmit/receive mode manually for these ports.		
	Port The LAN port number. Note: Do not change the automatic setting of Port 1,4 and Port 5 the Management 2 and Signaling 2 Networks. Any change to the speed of these ports will not be applied.		
	Speed	Select the speed and transmit/receive mode for each port. Default: Auto – Negotiation of speed and transmit/receive mode starts at 1000 Mbits/second Full Duplex, proceeding downward to 10 Mbits/second Half Duplex. Notes:	
		To maximize conferencing performance, especially in high bit rate call environments, a 1Gb connection is recommended.	
		RealPresence Collaboration Server (RMX) 4000 - Do not select 1000 Full Duplex for any LAN ports in Slot 17. Select only 100 Full Dupley.	
	 Select only 100 Full Duplex. RealPresence Collaboration Server (RMX) 1500 - Do not select 1000 Full Duplex for Port 5 (ShM). Select only 100 Full Duplex. 		
802.1x Authentication	For more information about 8.2.1x Authentication see IEEE 802.1X Authentication. Note: Ultra Secure Mode and these options are not supported with Collaboration Server 1800.		
User Name			
Password			

3 Click OK.

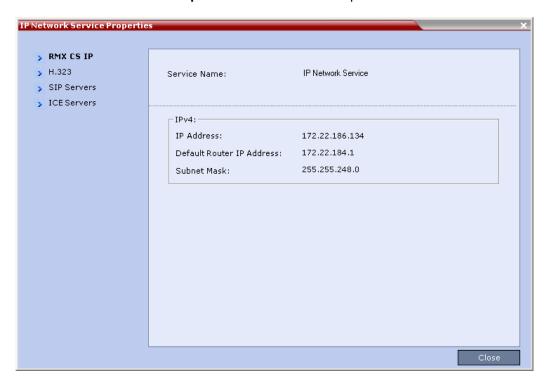
IP Network Monitoring

The **Signaling Monitor** is the Collaboration Server entity used for monitoring the status of external network entities such as the gatekeeper, DNS, SIP proxy and Outbound proxy and their interaction with the MCU.

To monitor signaling status:

- 1 In the RMX Management pane, click Signaling Monitor (-).
- 2 In the Signaling Monitor pane, double-click Default IP Service.

The IP Network Services Properties – RMX CS IP tab opens:



The **RMX CS IP** tab displays the following fields:

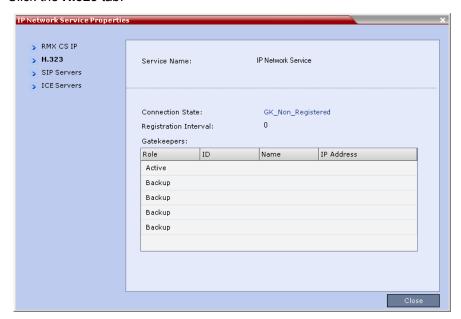
IP Network Services Properties - RMX CS IP Parameters

Field	Description
Service Name	The name assigned to the IP Network Service by the Fast Configuration Wizard.
	Note: This field is displayed in all tabs.

IP Network Services Properties – RMX CS IP Parameters

Field	Description			
IPv4	Default Router IP Address The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.			
			r the defined static routers are not able to to their destination. The default router is also	
	Subnet Mask	The subnet mask of the MCU. Default value: 255.255.255.0 .		
IPv6	Scope	IP Address		
		Global	The Global Unicast IP address of the Collaboration Server.	
		Site-Local	The IP address of the Collaboration Server within the local site or organization.	
	Default Router IP Address	The IP address of the default router. The default router is used whenever the defined static routers are not able to route packets to their destination. The default router is also used when host access is restricted to one default router.		

3 Click the H.323 tab.

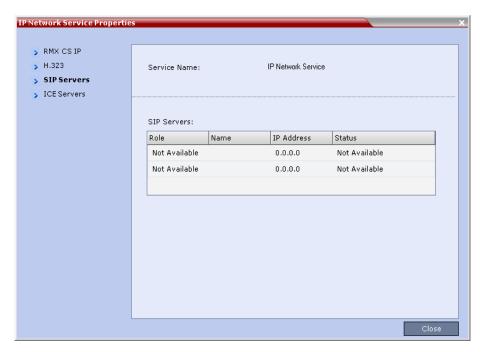


The **H.323** tab displays the following fields:

IP Network Services Properties - H.323 Parameters

Field	Description		
Connection State	The state of the connection between the Signaling Host and the gatekeeper: Discovery - The Signaling Host is attempting to locate the gatekeeper. Registration - The Signaling Host is in the process of registering with the gatekeeper. Registered - The Signaling Host is registered with the gatekeeper. Not Registered - The registration of the Signaling Host with the gatekeeper failed.		
Registration Interval	The interval in seconds between the Signaling Host's registration messages to the gatekeeper. This value is taken from either the IP Network Service or from the gatekeeper during registration. The lesser value of the two is chosen.		
	Role Active - The active gatekeeper. Backup - The backup gatekeeper that can be used if the connection to the preferred gatekeeper fails.		
	ID	The gatekeeper ID retrieved from the gatekeeper during the registration process.	
	Name	The gatekeeper's host's name.	
	IP Address	The gatekeeper's IP address.	

4 Click the SIP Servers tab.



The **SIP Servers** tab displays the following fields:

IP Network Services Properties - SIP Servers Parameters

Field	Description
Role	Active -The default SIP Server is used for SIP traffic. Backup -The SIP Server is used for SIP traffic if the preferred proxy fails.
Name	The name of the SIP Server.
IP Address	The SIP Server's IP address.
Status	The connection state between the SIP Server and the Signaling Host. Not Available - No SIP server is available. Auto - Gets information from DHCP, if used.

5 Click the ICE Servers tab.



The ICE Servers tab displays the following fields:

IP Network Services Properties – ICE Servers Parameters

Field	Description
Role	The ICE Server's role is displayed: STUN password server STUN Server UDP STUN Server TCP Relay Server UDP Relay Server TCP
IP Address	The ICE Server's IP Address.

IP Network Services Properties – ICE Servers Parameters

Field	Description
Status 1/2/3/4	A status is displayed for each media card installed in the Collaboration Server: Connection O.K. MS – register fail MS – subscribe fail MS – service fail Connection failed User/password failed Channel didn't receive any packets for 5 seconds Channel exceeded allotted bandwidth Unknown failure In systems with multiple media cards, Status 1 refers to the uppermost media card.
FW Detection	The Firewall Detection status is displayed: Unknown UDP enabled TCP enabled Proxy -TCP is possible only through proxy Block – both UDP & TCP blocked None

LAN Redundancy

LAN Redundancy enables the redundant LAN port connection to automatically replace the failed LAN port by using another physical connection and NIC (Network Interface Card). When a LAN port fails, IP network traffic failure is averted and network or endpoints disconnections do not occur. When LAN cables are connected to both LAN 1 and LAN 2 ports, the RMX automatically selects which port is active and which is redundant.

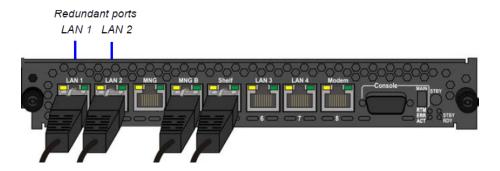
Media Redundancy

Media Redundancy on RealPresence Collaboration Server (RMX) 1500

On the RealPresence Collaboration Server (RMX) 1500 LAN 1 and LAN 2 are the redundant media ports:

- LAN 2 port is used for standard communications
- LAN 1 port can be used to define a second Network Service or for LAN Redundancy

RealPresence Collaboration Server (RMX) 1500 - RTM IP 1500 on Rear Panel



Media Redundancy on RealPresence Collaboration Server (RMX) 2000/4000

On the RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000, the LAN 1 and LAN 2 port on the RTM LAN card can be used as redundant media ports.

RealPresence Collaboration Server (RMX) 2000/ 4000 RTM LAN Card on Rear Panel



Media Redundancy on the RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000 is dependent on the settings of the **LAN_REDUNDANCY** and **MULTIPLE_SERVICES** System Flags as summarized in the following table:

RMX 1500 / 2000 / 4000 - Media Redundancy - System Flags

System Flag / Value	RMX 1500	RMX 2000	RMX 4000
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = NO		No Redundancy	
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = YES	No Redundancy		
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = NO	Full Redundancy	Media Redundancy Only	Full Redundancy
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = YES	Full Media Redundancy (If only one IP Network	Service is defined per m	edia card.)

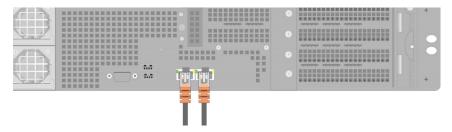
Media Redundancy is not supported on any of the RMX RTM ISDN cards.

Media and Signaling Redundancy on RealPresence Collaboration Server (RMX) 1800

On the RealPresence Collaboration Server 1800 LAN 1 and LAN 2 are the redundant media and signaling ports:

- LAN 1 port is used for standard communications
- LAN 2 port can be used to define a second Network Service or for LAN Redundancy

The following cables are connected to the LAN ports on the rear panel of the RealPresence Collaboration Server 1800:



LAN Connections to the IP ports

IP Port	Description
LAN 1	For management network connections: When LAN redundancy is enabled, LAN 1 is used for management, media, and signaling network connections.
LAN 2	For media, and signaling network connections: When LAN redundancy is enabled, LAN 2 is the backup for the LAN 1 port.

Media Redundancy on the RealPresence Collaboration Server (RMX) 1800 is dependent on the settings of the **LAN_REDUNDANCY** and **MULTIPLE_SERVICES** System Flags as summarized in the following table:

RMX 1800 - Media Redundancy - System Flags

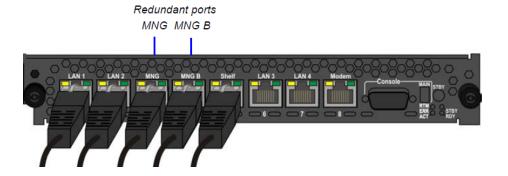
System Flag / Value	RMX 1800
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = NO	No Redundancy. If a second LAN cable is connected to Port 2, Network separation is enabled (the Management Network Service is separated from the Default IP Network Service)
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = YES	No Redundancy.
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = NO	Full Redundancy
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = YES	These flags cannot be set to YES simultaneously.

Signaling and Management Redundancy

Signaling and Management Redundancy on RealPresence Collaboration Server (RMX) 1500

On the RealPresence Collaboration Server (RMX) 1500, for Signaling and Management Redundancy, the **MNG** port is redundant to the **MNG** B port and must have a LAN cable connected.

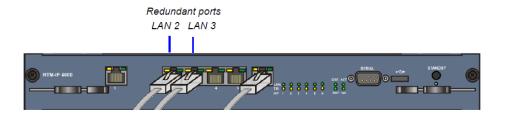
RealPresence Collaboration Server (RMX) 1500 - RTM IP 1500 on Rear Panel



Signaling and Management Redundancy on RealPresence Collaboration Server (RMX) 4000

On the RealPresence Collaboration Server (RMX) 4000, for Signaling and Management Redundancy when **LAN_REDUNDANCY** = **YES** and **MULTIPLE_SERVICES** = **NO**, the **LAN 3** port on the **RTM-IP 4000** card is redundant to the **LAN 2** port. **LAN** ports **4** and **5** are never used.

RealPresence Collaboration Server (RMX) 4000 - RTM IP 4000 on Rear Panel2



On the RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 4000 Signaling and Management Redundancy is implemented using the LAN ports on the RTM-IP card and is dependent on the settings of the **LAN_REDUNDANCY** and **MULTIPLE_SERVICES** System Flags as summarized in the following table.

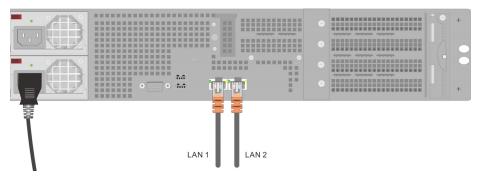
RMX 1500 / 4000 - Signaling and Management Redundancy - System Flags

	Port Usage		
Flag / Value	LAN 2 / MNG B (RMX 1500)	LAN 3 / MNG (RMX 1500)	
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = NO	Management	Signaling	
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = YES	Management	Not Used	
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = NO	Management & Signaling (LAN3 is redundant to LAN 2)		
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = YES	Management	Management	

Management Redundancy on RealPresence Collaboration Server (RMX) 1800

On the RealPresence Collaboration Server 1800, for Management Redundancy, the **LAN 2** port is redundant to the **LAN 1** port and must have a LAN cable connected.

RealPresence Collaboration Server 1800 - LAN 2 connection on Rear Panel



On the RealPresence Collaboration Server 1800, Management Redundancy is implemented using the **LAN** 1 and **LAN** 2 ports and is dependent on the settings of the **LAN_REDUNDANCY** and **MULTIPLE_SERVICES** System Flags as summarized in the following table.

RMX 1800 - Management Redundancy - System Flags

	Port Usage	
Flag / Value	LAN 1	LAN 2
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = NO	Management	Media and Signaling
LAN_REDUNDANCY = NO MULTIPLE_SERVICES = YES	Management	Media and Signaling
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = NO	Management, Media and Signaling.	LAN 2 is redundant to LAN 1
LAN_REDUNDANCY = YES MULTIPLE_SERVICES = YES	These flags cannot be set to YES simultaneously.	

Configuration Requirements

LAN Redundancy is disabled by default and is enabled by changing the **LAN_REDUNDANCY** system flag to **YES** and connecting the appropriate LAN cables to the LAN ports on the Collaboration Server as follows:

RealPresence Collaboration Server (RMX) 1500

Connect the additional LAN cable to LAN 1 port on the RTM IP.

RealPresence Collaboration Server 1800

• Connect the additional LAN cable to LAN 2 port on the rear panel of the Collaboration Server 1800.

RealPresence Collaboration Server (RMX) 2000



On a RealPresence Collaboration Server (RMX) 2000, one RTM LAN card is required. For more information see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide*, Installing or Replacing the RTM LAN.

- Connect the additional LAN cable to LAN 1 port on the RTM LAN.
- In the Setup> System Configuration > System Flags dialog box, add the flag RMX2000_RTM_LAN and set it to YES to activate the installed RTM LAN card.
- On the RealPresence Collaboration Server (RMX) 2000, LAN Redundancy can be enabled simultaneously with Multiple Networks. To enable the Multiple Networks option, set the MULTIPLE_SERVICES flag to YES.
- A system reset is required when adding the RMX2000_RTM_LAN flag.

RealPresence Collaboration Server (RMX) 4000

- Connect the additional LAN cable to LAN 1 port on the RTM LAN.
- On the RealPresence Collaboration Server (RMX) 4000, LAN Redundancy can be enabled simultaneously with Multiple Networks. To enable the Multiple Networks option, set the MULTIPLE_SERVICES flag to YES.
- If required, reset the Collaboration Server.

On all systems:

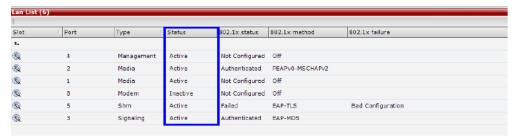
- LAN Redundancy can be disabled by setting the LAN_REDUNDANCY System Flag to NO.
- If the LAN_REDUNDANCY System Flag value set to NO, the LAN 2 port must be connected to the IP network.



On the RMX 1500/2000/4000, full media redundancy is supported if only one IP Network Service is defined per media card.

Hardware Monitor Indications

When LAN Redundancy is enabled on the Collaboration Server, LAN 2 port is **Active.** With LAN redundancy, when LAN LEDs are lit they indicate that a physical connection of the cables is present but does not indicate their activity status. In the **Hardware Monitor** pane the **Lan List** displays the Collaboration Server LAN ports together with their **Status** indication.



The Hardware Monitor Status indications are summarized in the following table:

RTM LAN Indications

Status	Description
Active	The LAN port cable is connected.
Inactive	The LAN port cable is not connected.
Standby	The LAN Redundancy option is enabled and this LAN port is the redundant and in standby mode. In case of failure, this port becomes active.

Network Traffic Control

The Network Traffic Control mechanism controls the level of UDP packets generated by the system. It regulates a set of queuing systems and mechanisms by which UDP packets are received and transmitted to the network router.

During a conference the MPMx cards occasionally blast-out UDP packets which can cause overloads on the network. Collaboration Server bandwidth usage can increase to above the designated conference participant line rate settings, causing network bandwidth issues such as latency and packet loss.



Only supported in the MPMx Card Configuration mode.

Three Network Traffic Control Flags are used to control the Network Traffic mechanism:

• ENABLE_TC_PACKAGE -

When the flag is set to **NO** (default), **Network Traffic Control** is disabled on the Collaboration Server. Set the flag to **YES** to enable Network Traffic Control.

• TC BURST SIZE -

This flag regulates the Traffic Control buffer or maxburst size as a percentage of the participant line rate. In general, higher traffic rates require a larger buffer. For example, if the flag is set to 10 and the participants line rate is 2MB, then the burst size is 200Kbps.

Default = 10

Flag range: 1-30.

• TC LATENCY SIZE -

This flag limits the latency (in milliseconds) or the number of bytes that can be present in a queue.

Default = 500

Flag range: 1-1000 (in milliseconds).

SIP Proxy Failover With Polycom® Distributed Media Application™ (DMA™) 7000

Collaboration Server systems that are part of a RealPresence DMA system environment can benefit from the RealPresence DMA system's SIP Proxy Failover functionality.

SIP Proxy Failover is supported in the RealPresence DMA system's Local Clustering mode with redundancy achieved by configuring two DMA servers to share a single virtual IP address.

The virtual IP address is used by the Collaboration Server as the IP address of its SIP Proxy.

No additional configuration is needed on the Collaboration Server.

Should a SIP Proxy failure occur in one of the RealPresence DMA system servers:

- The other RealPresence DMA system server takes over as SIP Proxy.
- Ongoing calls may be disconnected.
- Previously ongoing calls will have to be re-connected using the original IP address, registration and connection parameters.
- New calls will connect using the original IP address, registration and connection parameters.

RealPresence Collaboration Server (RMX) Network Port Usage

The following table summarizes the port numbers and their usage in the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000:

Server Network Port Usage Summary

Connection Type	Port Number	Protocol	Description	Configurable
НТТР	80	TCP	Management between the Collaboration Server and Collaboration Server Web Client.	No
HTTPS	443	TCP	Secured Management between the Collaboration Server and Collaboration Server Web Client.	No
DNS	53	UDP	Domain name server.	Can be disabled in the IP Network Service.
DHCP	68	UDP	Dynamic Host Configuration Protocol.	Can be disabled in the IP Network Service.
SSH	22	TCP	Secured shell. It is the Collaboration Server terminal. SSH is not supported when the Collaboration Server is in Ultra Secure Mode. For more information see Ultra Secure Mode.	No
NTP	123	UDP	Network Time Protocol. Enables access to a time server on the network.	No
H.323 GK RAS	1719	UDP	Gatekeeper RAS messages traffic.	No
H.323 Q.931	1720 - incoming; 49152-599 99 - outgoing	TCP	H.323 Q.931 call signaling. Each outgoing call has a separate port. The port for each outgoing call is allocated dynamically.	Yes - for outgoing calls only. It is configured in the Fixed Ports section of the IP service.
H.323 H.245	49152 - 59999	TCP	H.245 control. Each outgoing call has a separate port. The port for each outgoing call is allocated dynamically. It can be avoided by tunneling.	Yes - for outgoing calls only. It is configured in the Fixed Ports section of the IP service.

Server Network Port Usage Summary

Connection Type	Port Number	Protocol	Description	Configurable
SIP server	5060 60000	UDP, TCP	Connection to the SIP Server. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
Alternative SIP server	5060 60000	UDP, TCP	Connection to the alternate SIP Server. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
SIP Outbound proxy	5060 60000	UDP, TCP	Connection to the SIP outbound proxy. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
Alternative SIP Outbound proxy	5060 60000	UDP, TCP	Connection to the alternate SIP outbound proxy. Sometimes port 60000 is used when the system cannot reuse the TCP port. This port can be set in the Central signaling (CS) configuration file.	Yes - in the IP service.
SIP-TLS	60002	TCP	Required for Binary Floor Control Protocol (BFCP) functionality for SIP People+Content content sharing.	No - port is not opened if SIP People+Content is disabled.
RTP	49152 - 59999	UDP	RTP media packets. The ports are dynamically allocated.	Yes - It is configured in the Fixed Ports section of the IP service.
RTCP	49152 - 59999	UDP	RTP control. The ports are dynamically allocated.	Yes - It is configured in the Fixed Ports section of the IP service.
SIP -TLS	5061	TCP	SIP -TLS for SIP server, alternate SIP server, outbound proxy and alternate outbound proxy.	No

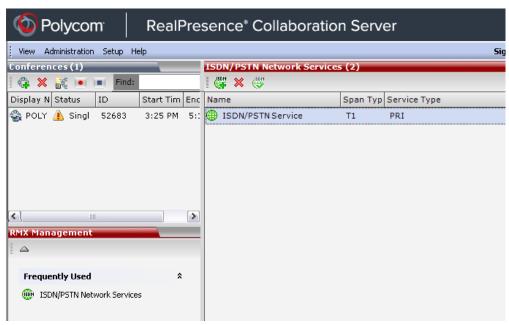
Defining ISDN/PSTN Network Services

To enable the RealPresence Collaboration Server (RMX) to function within ISDN/PSTN network environments, network parameters must be defined for the ISDN/PSTN Network Service.



ISDN and Gateway calls are not supported with RealPresence® Collaboration Server 1800 and any reference to these features relates to the RealPresence® Collaboration Server 1500/2000/4000.

The configuration dialog boxes for both this network services is accessed from the **RMX Management** pane of the RMX Web Client or RMX Manager.



IISDN/PSTN Network Services Overview

To enable ISDN and PSTN participants to connect to the MCU, an ISDN/PSTN Network Service must be defined. A maximum of two ISDN/PSTN Network Services, of the same Span Type (E1 or T1) can be defined for the Collaboration Server. Each Network Service can attach spans from either or both cards.

Most of the parameters of the first ISDN/PSTN Network Service are configured in the Fast Configuration Wizard, which runs automatically if an RTM ISDN card is detected in the Collaboration Server during first time power-up. For more information, see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Getting Started Guide, Procedure 1: First-time Power-up.

Supported Capabilities and Conferencing Features:

- ISDN video is supported only in **Continuous Presence** (CP) conferences.
- Only BONDING (using multiple channels as a single, large bandwidth channel) is supported.
- Simple audio negotiation.
- Supported video resolutions are the same as for IP.
- Supported video Protocols are the same as for IP: H.261, H.263, H.264.
- H.239 for content sharing.
- Lecture Mode.
- DTMF codes.
- Securing of conferences.
- Basic cascading between two MCUs using an ISDN link is available and forwarding of DTMF codes can be suppressed.

Non Supported Capabilities and Conferencing Features:

- NFAS (Non-Facility Associated Signaling)
- Leased line usage
- Restricted Channel mode
- Aggregation of channels
- V.35 serial standards
- Primary and secondary clock source configuration (they are automatically selected by the system)
- Auto detection of Audio Only setting at endpoint
- Auto re-negotiation of bit rate
- Additional network services (two currently supported)
- Change of video mode (capabilities) from remote side during call
- Audio algorithms G.729 and G.723.1
- FECC
- H.243 Chair Control
- T.120 data sharing protocol
- H.261 Annex D
- MIH Cascading using an ISDN connection as cascade link

Adding/Modifying ISDN/PSTN Network Services

The system administrator can use the RMX Management – ISDN/PSTN Network Services section of the Collaboration Server Web Client to add a second ISDN/PSTN Network Service or modify the first ISDN/PSTN Network Service.



A new ISDN/PSTN Network Service can be defined even if no RTM ISDN card is installed in the system.

Obtaining ISDN/PSTN required information

Before configuring the ISDN/PSTN Network Service, obtain the following information from your ISDN/PSTN Service Provider:

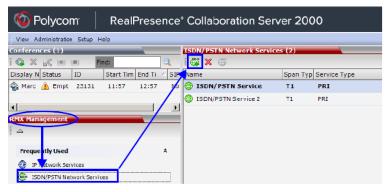
- Switch Type
- Line Coding and Framing
- Numbering Plan
- Numbering Type
- Dial-in number range



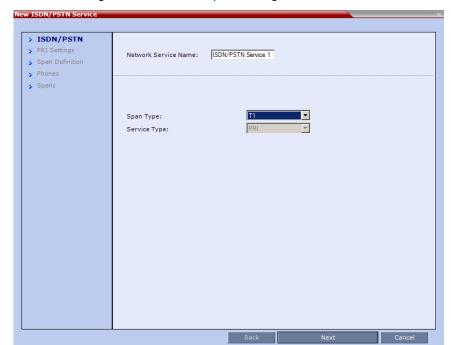
If the Collaboration Server is connected to the public ISDN Network, an external CSU or similar equipment is needed.

To Add an ISDN/PSTN Network Service:

1 In the RMX Management pane, click ISDN/PSTN Network Services (66).



2 In the ISDN/PSTN Network Services list menu, click New ISDN/PSTN Service (), or right-click anywhere in the ISDN/PSTN Network Services list and select New ISDN/PSTN Service.



The Fast Configuration Wizard sequence begins with the **ISDN/PSTN** dialog box:

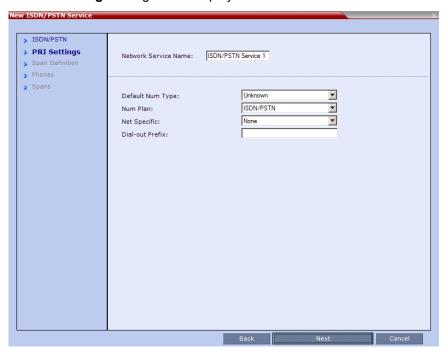
3 Define the following parameters:

ISDN Service Settings

Field	Description
Network Service Name	Specify the service provider's (carrier) name or any other name you choose, using up to 20 characters. The Network Service Name identifies the ISDN/PSTN Service to the system. Default name: ISDN/PSTN Service Note: This field is displayed in all ISDN/PSTN Network Properties tabs and can contain character sets that use Unicode encoding.
Span Type	Select the type of spans (ISDN/PSTN) lines, supplied by the service provider, that are connected to the Collaboration Server. Each span can be defined as a separate Network Service, or all the spans from the same carrier can be defined as part of the same Network Service. Select either: • T1 (U.S. – 23 B channels + 1 D channel) • E1 (Europe – 30 B channels + 1 D channel) Default: T1
Service Type	PRI is the only supported service type. It is automatically selected.

4 Click Next.

The **PRI Settings** dialog box is displayed:



5 Define the following parameters:

ISDN Service Settings

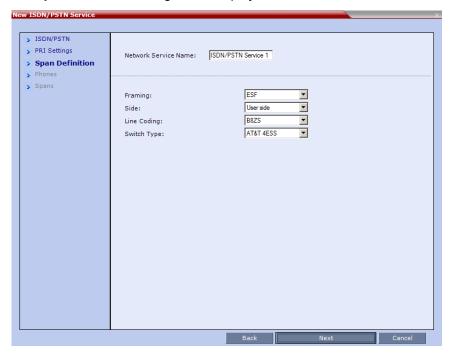
Field	Description
Default Num Type	Select the Default Num Type from the list.
	The Num Type defines how the system handles the dialing digits. For example, if you type eight dialing digits, the Num Type defines whether this number is national or international.
	If the PRI lines are connected to the Collaboration Server via a network switch, the selection of the Num Type is used to route the call to a specific PRI line. If you want the network to interpret the dialing digits for routing the call, select Unknown .
	Default: Unknown
	Note: For E1 spans, this parameter is set by the system.
Num Plan	Select the type of signaling (Number Plan) from the list according to information given by the service provider. Default: ISDN
	Note: For E1 spans, this parameter is set by the system.
Net Specific	Select the appropriate service program if one is used by your service provider (carrier).
	Some service providers may have several service programs that can be used. Default: None

ISDN Service Settings

Field	Description
Dial-out Prefix	Enter the prefix that the PBX requires to dial out. Leave this field blank if a dial-out prefix is not required.
	The field can contain be empty (blank) or a numeric value between 0 and 9999 . Default: Blank

6 Click Next.

The **Span Definition** dialog box is displayed:



7 Define the following parameters:

Span Definition

Field	Description
Framing	Select the Framing format used by the carrier for the network interface from the list. • For T1 spans, default is SFSF . • For E1 spans, default is FEBE .

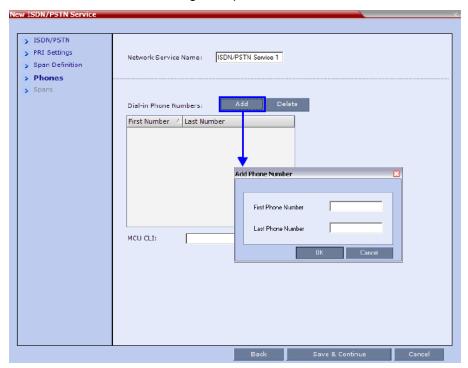
Span Definition

Field	Description
Side	Select one of the following options: User side (default) Network side Symmetric side Note: If the PBX is configured on the network side, then the Collaboration Server unit must be configured as the user side, and vice versa, or both must be configured symmetrically.
Line Coding	 Select the PRI line coding method from the list. For T1 spans, default is B8ZS. For E1 spans, default is HDB3.
Switch Type	Select the brand and revision level of switch equipment installed in the service provider's central office. • For T1 spans, default is AT&T 4ESS . • For E1 spans, default is EURO ISDN . Note: For T1 configurations in Taiwan, Framing must be set to ESF and Line Coding to B8ZS .

8 Click Next.

The **Phones** dialog is displayed.

- **9** To define dial-in number ranges click the **Add** button.
- 10 The Add Phone Number dialog box opens.



11 Define the following parameters:

Phones Settings

Field	Description
First Number	The first number in the phone number range.
Last Number	The last number in the phone number range.



- A range must include at least two dial-in numbers.
- A range cannot exceed 1000 numbers.

12 Click OK.

The new range is added to the **Dial-in Phone Numbers** table.

- 13 To define additional dial-in ranges, repeat steps 8 to 10.
- 14 Enter the MCU CLI (Calling Line Identification).

In a dial-in connections, the **MCU CLI** indicates the MCU's number dialed by the participant. In a dial-out connection, indicates the MCU (CLI) number as seen by the participant

15 Click Save & Continue.

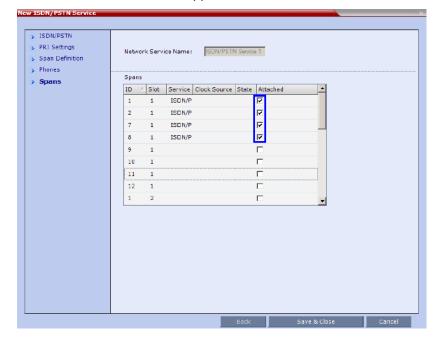
After clicking **Save & Continue**, you cannot use the **Back** button to return to previous configuration dialog boxes.

The ISDN/PSTN Network Service is created and confirmed.

16 Click **OK** to continue the configuration.

The **Spans** dialog box opens displaying the following read-only fields:

- ▶ ID The connector on the ISDN/PSTN card (PRI1 PRI12).
- > Slot The media card that the ISDN/PSTN card is connected to (1 or 2)
- Service The Network Service to which the span is assigned, or blank if the span is not assigned to a Network Service
- ➤ Clock Source Indicates whether the span acts as a clock source, and if it does, whether it acts as a Primary or Backup clock source. The first span to synchronize becomes the primary clock source.
- > State The type of alarm: No alarm, yellow alarm or red alarm.
- 17 Attach spans to existing Network Services, by marking the appropriate check boxes in the Attached field.



Each ISDN/PSTN card can support 7 E1 or 9 T1 PRI lines.

18 Click Save & Close.

Modifying an ISDN/PSTN Network Service

To Modify an ISDN/PSTN Network Service:

- 1 In the RMX Management pane, click ISDN/PSTN Network Services ().
- 2 In the ISDN/PSTN Network Services list, double-click the ISDN or right-click the ISDN entry and select Properties.

The ISDN Properties dialog boxes are displayed. They are similar to the Fast Configuration Wizard's dialog boxes. For more information see Adding/Modifying ISDN/PSTN Network Services .

The following **ISDN Properties** can be modified:

- > PRI Settings
 - ♦ Net Specific
 - ♦ Dial-out Prefix
- > Span Definition
 - Framing
 - ♦ Side
 - Line Coding
 - Switch Type
- Phones
 - Dial-in Phone Numbers
 - **♦ MCU CLI**

> Spans

♦ Attached

All other **ISDN Properties** can only be modified by deleting the ISDN/PSTN network service and creating a new PSTN service using the Fast Configuration Wizard. For more information, see Adding/Modifying ISDN/PSTN Network Services .

Network Security

System security can be enhanced by separating the Media, Signaling and Management Networks.

RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 4000

On the RealPresence Collaboration Server (RMX) 1500 and RealPresence Collaboration Server (RMX) 4000, Media, Signaling and Management Networks are physically separated to provide enhanced security. The Default IP Network Service and the Management Network Service have been logically and physically separated from each other. In the IP Network Service each IP address is assigned a physical port and media (RTP) inputs are routed directly to a media card. This provides for a more secure network with greater bandwidth as each media card has its own dedicated port. All signaling communications are processed on a single stack of the processor in the Collaboration Server.

RealPresence Collaboration Server 1800

On the RealPresence Collaboration Server 1800 the Default IP Network Service and the Management Network Service have been logically and physically separated from each other to provide enhanced security. The Collaboration Server 1800 includes two LAN ports that can be used for separating the management network from the signaling and media network or if Multiple Networks option is enabled, each LAN port is used for signaling, media and management per Network Service.

RealPresence Collaboration Server (RMX) 2000

On the RealPresence Collaboration Server (RMX) 2000 a RTM LAN or RTM ISDN card is required to enable the separation between the networks. By defining Multiple Network Services, a separate network can be defined for each media card installed in the system.

For more information see the *RealPresence Collaboration Server (RMX)* 1500/2000/4000 Deployment Guide for Maximum Security Environments, Procedure 5: Enable Network Separation (RMX 2000).

Multiple Network Services

Media, signaling and management networks can be physically separated on the Collaboration Server system to provide enhanced security. This addresses the requirement in an organization that different groups of participants be supported on different networks. For example, some participants may be internal to the organization while others are external.

Up to eight media and signaling networks can be defined for the RealPresence Collaboration Server (RMX) 4000, or four for the RealPresence Collaboration Server (RMX) 2000 and two for the RealPresence Collaboration Server (RMX) 1500/1800.

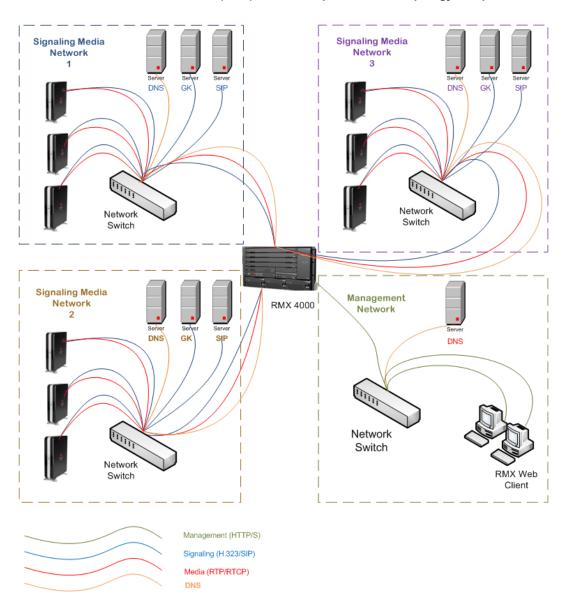
Multiple IP Network Services can be defined; up to two for each media and signaling network connected to the Collaboration Server. The networks can be connected to one or several Media cards in the Collaboration Server unit.

The Management Network is logically and physically separated from the media and signaling networks. There can be one Management Network defined per Collaboration Server system.

Each conference on the Collaboration Server can host participants from the different IP Network networks simultaneously.

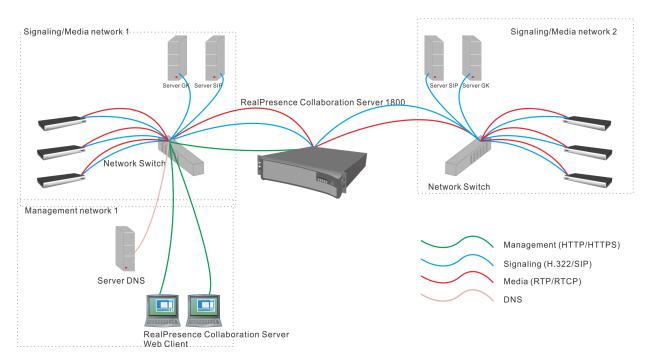
The following figure shows the network topology with three different media and signaling networks and one Management network connected to the Collaboration Server (RMX) 4000.

RealPresence Collaboration Server (RMX) 4000 - Multiple Networks Topology Sample



The following figure shows the network topology with two different media and signaling networks and one Management network connected to the Collaboration Server (RMX) 1800.

RealPresence Collaboration Server (RMX) 1800 - Multiple Networks Topology Sample



Guidelines

- Multiple Services system mode is a purchasable option and it is enabled in the MCU license.
- Multiple Network Services are supported in MCUs with at least 1024MB memory only. MCU units with memory of 512MB support only one IP Network Service.
- Multiple Services system mode is enabled when the system configuration flag MULTIPLE_SERVICES is added and set to YES.
- Only IPv4 is supported for the definition of Multiple Network Services.



The MULTIPLE_SERVICE System Flag cannot be set to YES when IPv6 Addressing is enabled.

- When configuring Multiple Networks on the RealPresence Collaboration Server (RMX) 2000, the RMX2000_RTM_LAN flag must be set to YES in addition to the MULTIPLE_NETWORKS=YES flag.
- Multiple Network Services are not supported with Microsoft ICE Environments in versions prior to Version 7.8.
- Up to two Network Services, one per LAN port, can be associated with each Media card.
- An IP Network Service can be associated with one or several media cards. If more than one card is
 associated with the same Network Service, the system routes the calls to the appropriate card
 according to resource availability.

- On the RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000, both RTM ISDN or RTM LAN can be used for Multiple Services configuration. However, if RTM ISDN is installed and used for Multiple Services configuration, only one Network Service can be associated with the media card to which the RTM ISDN card is attached.
- On the RealPresence Collaboration Server (RMX) 1500, when Multiple Network Services option is enabled, the two networks must differ in their subnet masks.
- On the RealPresence Collaboration Server (RMX) 1500 and 1800, LAN redundancy cannot be enabled in parallel to Multiple Networks and the LAN_REDUNDANCY flag must be set to NO when the Multiple Networks option is enabled.
- Participants on different networks can connect to the same conference with full audio, video and content capabilities.
- Traffic on one network does not influence or affect the traffic on other networks connected to the same MCU, unless they are connected to the same media card. If one network fails, it will not affect the traffic in the other connected networks, unless they are connected to the same media card and the card fails.
- Maximum number of services that can be defined per Collaboration Server platform:

Maximum Number of Network Services per Collaboration Server System

MCU	Total Media Cards	Network Services (Up to 2 per Media Card)	Management Services	Network Services that Include ICE (1 / Media Card)
1500	1	Up to 2	1	1
1800	3 (DSP Cards)	Up to 2	1	1
2000	2	Up to 4 when using 2 RTM LAN cards. Less when using a combination of RTM ISDN and RTM LAN, or 2 RTM ISDN cards.	1	2
4000	4	Up to 8 when using 4 RTM LAN cards. Less when using up to 2 RTM ISDN cards and the remaining RTM LAN cards.	1	4

- From Version 7.8 onwards, a DNS server can be specified for each IP Network Service and for the Collaboration Server Management Network Service.
 - ➤ In the Network Services that do not include the DNS, use the IP addresses of the various devices to define them in the Network Services.



DNS configuration is not applicable to the RealPresence Collaboration Server (RMX) 1800.

Participants are associated with a Network Service and use it resources as follows:

- Dial-in participants according to the network used to place the call and connect to the Collaboration Server.
- Dial-out participant according to the Network Service selected during the participant properties definition or during conference definition, according to the Network Service selected as default.
- Recording Links use the default Network Service to connect to conferences, therefore the recording system must be defined on the default network to enable the recording.

Resource Allocation and Capacity

The Video/Voice Port Configuration (Collaboration Server 1500/20000/4000 in MPMx Card Configuration Mode only) and the Resolution Configuration settings are configured per MCU and affect the resource capacity of the MCU. They are reflected in the port gauges displayed on the Collaboration Server management application's main screen. In Multiple Networks mode, the overall resources are divided between the Network Services. However, the port gauges do not reflect the resource availability per Network Service. For more information see Resource Capacity.

First Time Installation and Configuration

First Time Installation and Configuration of the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 consists of the following procedures:

- 1 Preparations:
 - Gather Network Equipment and Address Information Get the information needed for integrating the Collaboration Server into the local network for each of the networks that will be connected to the Collaboration Server.
 - Unpack the Collaboration Server.
 - Modify the Management Network parameters on the USB Key.
- 2 Hardware Installation and Setup:
 - Mount the Collaboration Server in a rack.
 - Connect the necessary cables.
- 3 First Entry Power-up and Configuration:
 - Power up the Collaboration Server.
 - Register the Collaboration Server.
 - Connect to the Collaboration Server.
 - Configure the Default IP Network Service.
 - Optional. For Models 1500/2000/4000, Configure the ISDN/PSTN Network Service.
 - Modify the required System Flag to enable Multiple Services and reset the MCU.
- 4 Add the required IP Network Services to accommodate the networks connected to the Collaboration Server.
- 5 Select a Network Service to act as default for dial out and gateway calls for which the Network Service was not selected.
- 6 Place several calls and run conferences to ensure that the system is configured correctly.

For details see the RMXTM 1800 Getting Started Guide. First Time Installation and Configuration.

Upgrading to Multiple Services

- 1 Gather Network Equipment and Address Information for each of the networks that will be connected to the Collaboration Server unit. For a list of required address, see the *RMX™* 1800 Getting Started Guide, Gather Network Equipment and Address Information.
- 2 Upgrade to the new version and install the activation key that contains the Multiple Services license as described in the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Release Notes.
- 3 Place several calls and run conferences to ensure that the system upgrade was completed successfully.
- 4 Modify the required System Flag to enable Multiple Services, DO NOT reset the MCU yet.
- 5 Connect the additional network cables to the Collaboration Server and change existing connections to match the required configuration as described in the appropriate RealPresence Collaboration Server (RMX) Hardware Guide.

At this point, the Management Network can be modified to match the required local network settings



If the RealPresence Collaboration Server (RMX) 2000 you are upgrading does not include RTM ISDN or RTM LAN cards, you must install at least one RTM LAN card to enable the definition of multiple Network Services. If no RTM ISDN or RTM LAN cards are installed, the RealPresence Collaboration Server (RMX) 2000 works in a single Network Service mode and an alarm is issued by the system. For more details about the installation of RTM LAN cards, see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide*.

- 6 Reset the MCU.
- 7 Connect to the MCU and add the required IP Network Services to accommodate the networks connected to the Collaboration Server unit.
- 8 Select a Network Service to act as default for dial out and gateway calls for which the Network Service was not selected.
- 9 Place several calls and run conferences to ensure that the system is configured correctly.

Gather Network Equipment and Address Information - IP Network Services Required Information

It is important that before connecting multiple networks and implementing Multiple Services in the Collaboration Server, that you obtain the information needed to complete the IP Network Service configuration for each connected network from your network administrator.

Network Equipment and Address Information per IP Network Service

Parameter	Local Network Settings	Note
Signaling Host IP address		
Media Board IP address (MPM 1)		

Network Equipment and Address Information per IP Network Service

Parameter	Local Network Settings	Note
Media Board IP address (MPM 2) RealPresence Collaboration Server (RMX) 2000/RealPresence Collaboration Server (RMX) 4000 only		If more than one media card is associated with this Network Service
Media Board IP address (MPM 3) RealPresence Collaboration Server (RMX) 4000 only		If more than one media card is associated with this Network Service
Media Board IP address (MPM 4) RealPresence Collaboration Server (RMX) 4000 only		If more than one media card is associated with this Network Service
Gatekeeper IP address (optional)		
DNS IP address (optional)		Only one DNS can be defined for the entire Network topology
SIP Server IP address (optional)		

RealPresence Collaboration Server (RMX) Hardware Installation

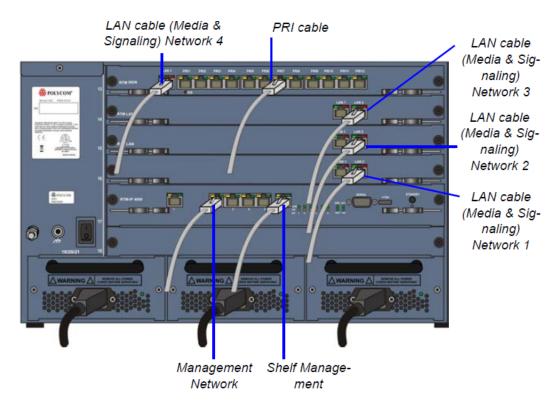


When connecting the LAN cables of the various networks to the Collaboration Server it is recommended to use a color system to differentiate between the networks, for example, using colored cables.

RealPresence Collaboration Server (RMX) 4000 Multiple Services Configuration

RealPresence Collaboration Server (RMX) 4000 Rear Panel with LAN and PRI cables shows the cables connected to the RealPresence Collaboration Server (RMX) 4000 rear panel, when one RTM ISDN and three RTM LAN cards are installed providing IP and ISDN connectivity. The RTM ISDN card can be used for both ISDN and IP calls and only one IP network Service is associated with each RTM LAN card.

RealPresence Collaboration Server (RMX) 4000 Rear Panel with LAN and PRI cables



In this case, up to four different IP Network Services can be defined - one for each RTM LAN/RTM ISDN cards installed in the system.

If two LAN ports per each installed RTM LAN card are used, up to three additional Network Services can be defined, bringing it to a total of up to 7 IP Network Services.

Several cards can be assigned to the same IP Network Service. The definition of the network services attached to the Collaboration Server unit and which cards are assigned to each network service is defined in the IP Network Service.

Connecting the cables to the RTM IP 4000:

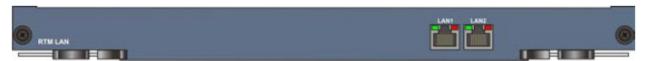
The following cables are connected to the RTM IP on the rear panel of the RealPresence Collaboration Server (RMX) 4000:



LAN Connections to the RTM IP

RTM IP Port	Description
LAN 1	Modem
LAN 2	Management
LAN 3	-
LAN 4	-
LAN 5	-
LAN 6	Shelf Management

Connecting the cables to the RTM LAN:



LAN Connections to the RTM LAN

RTM LAN Port	Description	
LAN 1	Signaling and Media - additional (second) Network Service	
LAN 2	Signaling and Media - existing (first) Network Service	

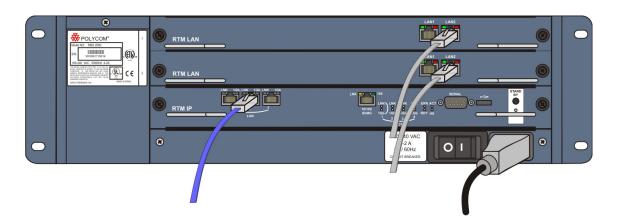
RealPresence Collaboration Server (RMX) 2000 Multiple Services Configuration

If one LAN port per RTM ISDN/ RTM LAN card is used, up to two different IP Network Services can be defined - one for each installed RTM LAN/RTM ISDN cards.

If two LAN ports per each installed RTM LAN card are used, up to four Network Services can be defined.

RealPresence Collaboration Server (RMX) 2000 Rear Panel with RTM LAN Cables shows the cables connected to the RealPresence Collaboration Server (RMX) 2000 rear panel, when two RTM LAN cards are installed providing IP connectivity. In this case, only one IP network Service can be associated with each RTM LAN card.

RealPresence Collaboration Server (RMX) 2000 Rear Panel with RTM LAN Cables



Connecting the cables to the RTM IP:

The following cables are connected to the RTM IP on the rear panel of the RealPresence Collaboration Server (RMX) 2000:



LAN Connections to the RTM IP

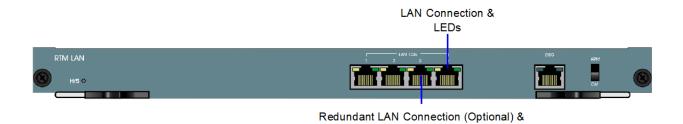
RTM IP Port	Description
LAN 1	-
LAN 2	Management
LAN 3	Modem

Connecting the cables to the RTM LAN:



If RTM LAN or RTM ISDN cards are not installed on the Collaboration Server, they must be installed before connecting the additional network cables for media and signaling.

LEDs



LAN Connections to the RTM LAN

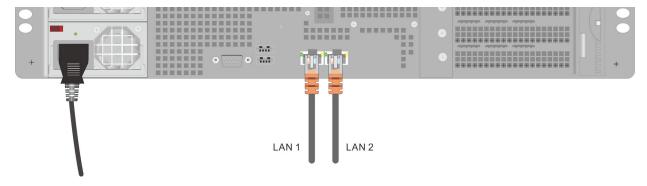
RTM IP Port	Description			
LAN 1	Signaling and Media - second Network Service (optional)			
LAN 2	Signaling and Media - first Network Service (optional)			

RealPresence Collaboration Server (RMX) 1800 Multiple Services Configuration

Up to two media and signaling networks can be defined for the RealPresence Collaboration Server (RMX) 1800. Each of these networks can be assigned a different IP Network Services (Multiple IP Network Services).

Connecting the cables to the RealPresence Collaboration Server 1800:

Two LAN cables are connected to the LAN ports on the rear panel of the RealPresence Collaboration Server 1800:



LAN Connections to the IP ports

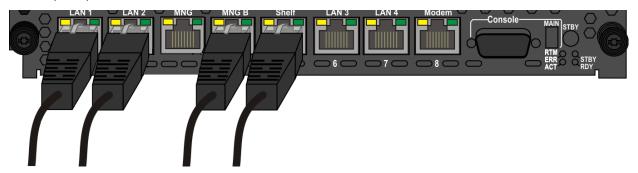
IP Port	Description			
LAN 1	Management, media and signaling for Network Service 1.			
LAN 2	Media and signaling for Network Service 2.			

RealPresence Collaboration Server (RMX) 1500 Multiple Services Configuration

Up to two media and signaling networks can be defined for the RealPresence Collaboration Server (RMX) 1500. Each of these networks can be assigned a different IP Network Services (Multiple IP Network Services).

Connecting the cables to the RTM IP 1500:

The following cables are connected to the RTM IP on the rear panel of the RealPresence Collaboration Server (RMX) 1500:



LAN Connections to the RTM IP

RTM IP Port	Description			
LAN 1	Media and signaling - additional (second) Network Service			
LAN 2	Media and signaling - existing (first) Network Service			
MNG	-			
MNG B	Management			
Shelf	Shelf Management			
LAN 3	-			
LAN 4	-			
Modem	Modem			

Collaboration Server Configuration

Once the network cables are connected to the Collaboration Server, you can modify the default IP Network Service and add additional Network Services.

System Flags and License Settings

The **MULTIPLE_SERVICES** System Flag determines whether the Multiple Services option will be activated once the appropriate license is installed. Possible Values: **YES / NO** Default: **NO**

This flag must be manually added to the system configuration and set to **YES** to enable this option. For more information see Manually Adding and Deleting System Flags.



If the **MULTIPLE_SERVICES** System Flag is set to **YES** and no RTM ISDN or RTM LAN card is installed in the RealPresence Collaboration Server (RMX) 2000, an Active Alarm is displayed.

IP Network Service Definition

Use this procedure to define Network Services in addition to the Network Service already defined during first entry installation and configuration. Each of the defined Network Service can be associated with one or more media cards installed in the system (depending on the system type).

Once a media card is associated with a Network Service it cannot be associated with another network service.

To add new/additional Network Services:

- 1 In the Device Management pane, click IP Network Services (@).
- 2 In the Network Services list toolbar, click the Add Network Service button.

The New IP Service - Networking IP dialog box opens.

3 Define the following fields:

IP Network Service - IP Parameters

Field	Description				
Network Service Name	Enter the IP Network Service name. Note: This field is displayed in all IP Signaling dialog boxes and can contain character sets that use Unicode encoding.				
IP Network Type	Select the IP Network environment. You can select: H.323 - For an H.323-only Network Service. SIP - For a SIP-only Network Service. H.323 & SIP - For an integrated IP Service. Both H.323 and SIP participants can connect to the Collaboration Server using this service. Note: This field is displayed in all Default IP Service tabs.				

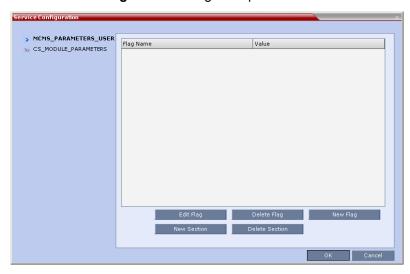
IP Network Service - IP Parameters

Field	Description				
Signaling Host IP Address	Enter the address to be used by IP endpoints when dialing into the Collaboration Server using this Network Service. Dial out calls of participants to whom this network service will be assigned are initiated from this address. This address is used to register the Collaboration Server with a Gatekeeper or a SIP Proxy server residing on this network.				
Media Card 1 Port 1 IP Address Media Card 1 Port 2 IP Address 2	If only one network is connected to this media card, it is enough to assign one media card to this Network Service. In such a case, enter one IP address for the media card according to the LAN Port used for the connection. If each of the LAN ports on one media card is used with two different networks, each port is assigned to its own Network Service. In such a case, enter the IP address of the port to be assigned to this Network Service. A LAN port that is already assigned to a different Network Service, displays the IP Address of the assigned port and it cannot be assigned to this Network Service (it is disabled).				
Media Card 2 Port 1 IP Address Media Card 2 Port 2 IP Address (RealPresence Collaboration Server (RMX) 2000/RealPresen ce Collaboration Server (RMX) 4000) Media Card 3 Port 1 IP Address/ Media Card 3 Port 2 IP Address (RealPresence Collaboration Server (RMX) 4000)	If only one network is connected to this media card, it is enough to assign one media card to this Network Service. In such a case, enter one IP address for the media card according to the LAN Port used for the connection, as provided by the network administrator. If each of the LAN ports on one media card is used with two different networks, each port is assigned to its own Network Service. In such a case, enter the IP address of the port to be assigned to this Network Service. Notes: LAN Ports/Media cards that are already associated with another Network Service cannot be associated with this Network Service. You can define a Network Service without assigning media cards to it. To change the assignment of a card from one service to another, the card must first be removed from the service to which it is assigned prior to its assignment to another service. RealPresence Collaboration Server (RMX) 2000: If one card was already assigned to another service, only one additional card can be assigned to this service. RealPresence Collaboration Server (RMX) 4000: Depending on the number of media cards installed in the system, you can assign up to 4 media cards to this				
Media Card 4 Port 1 IP Address Media Card 4 Port 2 IP Address (RealPresence Collaboration Server (RMX) 4000)	network service provided that they are not assigned to any other Network Service.				
Subnet Mask	Enter the subnet mask of the Collaboration Server in that network service. Default value: 255.255.255.0 .				

4 Optional. Some system flags can be defined per Network Service, depending on the network environment.

To modify these flags, click the **Service Configuration** button.

The Service Configuration dialog box opens.



All the flags must be manually added to this dialog box. For a detailed description of the flags and how to add them, see Manually Adding and Deleting System Flags.



Flags defined per Network Service override their general definition in the System Configuration.

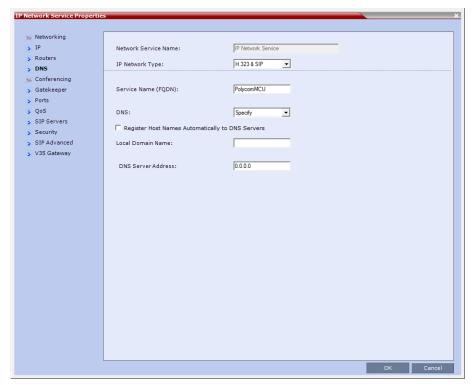
The following flags can be defined per service:

- ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF
- ➤ ENABLE_H239
- > SIP_ENABLE_FECC
- ENABLE_CLOSED_CAPTION
- ALLOW_NON_ENCRYPT_RECORDING_LINK_IN_ENCRYPT_CONF
- NUMERIC_CONF_ID_LEN
- NUMERIC_CONF_ID_MIN_LEN
- NUMERIC_CONF_ID_MAX_LEN
- > ENABLE_CASCADED_LINK_TO_JOIN_WITHOUT_PASSWORD
- MAX_CP_RESOLUTION
- QOS_IP_AUDIO
- QOS_IP_VIDEO
- QOS_IP_SIGNALING
- > ENABLE_CISCO_GK
- > SIP_FREE_VIDEO_RESOURCES

- FORCE_CIF_PORT_ALLOCATION
- MS_ENVIRONMENT
- SIP_FAST_UPDATE_INTERVAL_ENV
- > SIP_FAST_UPDATE_INTERVAL_EP
- > H263_ANNEX_T
- > H239 FORCE CAPABILITIES
- > MIX_LINK_ENVIRONMENT
- > IP_LINK_ENVIRONMENT
- > FORCE_STATIC_MB_ENCODING
- > FORCE_RESOLUTION
- > SEND_WIDE_RES_TO_IP
- DISABLE_WIDE_RES_TO_SIP_DIAL_OUT
- > SEND_SIP_BUSY_UPONRESOURCE_THRESHOLD
- 5 Click the Routers tab.
- Define the routers used in this network and that are other than the routers defined in the Management Network. The field definitions of the Routers tab are the same as for the Default Management Network. For more information see Default Management Network Service Routers.
- 7 Click the **DNS** tab.



DNS configuration is not applicable to the RealPresence Collaboration Server (RMX) 1800.



8 Modify the following fields:

Default Management Network Service - DNS

Field	Description				
Service Host Name	Enter the host name of this network Service. Each Network Service must have a unique Host Name otherwise an error message is displayed.				
DNS	 Select: Off – If no DNS server is used in this network. Specify – To enter the IP address of the DNS server used by this network service. Notes: The IP address field is enabled only if Specify is selected. In both Standard Security and Ultra Secure Modes: A DNS can be configured for the Management Network Service that is defined and the IP Network Service. If a Multiple Services Licence is installed, a DNS can be configured for each additional IP Network Service that is defined. If the DNS field in the IP Network Service is set to Specify and the DNS is not configured or disabled, the DNS configured for the Management Network will be used. When upgrading from a version that does not support a DNS per IP Network Service, the DNS configured for the Management Network will be used. 				

Default Management Network Service - DNS

Field	Description		
Register Host Names Automatically to DNS Servers	Select this option to automatically register this Network Service Signaling Host with the DNS server.		
Local Domain Name	Enter the name of the domain for this network service.		
DNS Server Address	Enter the static IP address of the DNS server that is part of this network.		

9 Click the Gatekeeper tab.

10 Define the Primary and Alternate Gatekeepers and at least one Alias for this network Service. The field definitions of the Gatekeeper tab are the same as for the Default IP Network Service. For more information see Default IP Service – Conferencing – Gatekeeper Parameters.



In **Multiple Services** mode, an Alias must be defined for the specified gatekeeper.

11 To view or modify the port settings, click the **Ports** tab.

Settings in the Ports tab allow specific ports in the firewall to be allocated to multimedia conference calls. If required, defined the ports to be used multimedia conference calls handled by this Network Service. The field definitions of the Ports tab are the same as for the Default IP Network Service.

For more information see Default IP Service – Conferencing – Ports Parameters.

12 If required, click the QoS tab.

The Collaboration Server's implementation of **QoS** is defined per Network Service, not per endpoint.



The routers must support QoS in order for IP packets to get higher priority.

The field definitions of the QoS tab are the same as for the Default IP Network Service. For more information see Default IP Service – Conferencing – QoS Parameters.

- 13 Click the SIP Servers tab.
- **14** Define the **Primary** and **Alternate SIP Server** for this network Service.



- Starting with Version 7.1, Registration of conferencing entities with the SIP Servers was moved to the conferencing entities and is defined in the Conference Profile.
- If Microsoft Office Communications or Lync server are part of this network service, a certificate
 must be created for this network service. If each network connected to the Collaboration Server
 includes Microsoft Office Communications or Lync server, separate certificates must be created
 and sent to the Collaboration Server for each of these networks.
- If the Network Service does not include a DNS, you must use the IP address of the SIP Server instead of its name.

The field definitions of the **SIP Servers** tab are the same as for the **Default IP Network Service**. For more information see Default IP Network Service – SIP Servers.

15 Click the Security tab.

The field definitions of the Security tab are the same as for the Default IP Network Service. For more information see Default IP Network Service – Security (SIP Digest).

- **16** To configure the ICE environment, click the **SIP Advanced** tab.
- **17** Modify the following fields:

Default IP Network Service - SIP Advanced

Field	Description			
Server User Name	Enter the User name for this service as defined in the Active Directory . For example, enter rmxNet2 . This field is disabled if the ICE Environment field is set to None .			
ICE Environment	Select MS (for Microsoft ICE implementation) to enable the ICE integration. This field is disabled if the Collaboration Server is not running in MPM+ Card Configuration Mode .			

18 Click the OK button.

The new Network Service is added to the IP Network Services list pane.

Setting a Network Service as Default

The default Network Service is used when no Network Service is selected for the following:

- Dial out participants
- Reserving resources for participants when starting an ongoing conference
- Gateway calls

In addition, the Signaling Host IP address and the MCU Prefix in GK displayed on the Collaboration Server Web Client main screen are taken from the default H.323 Network Service.

One IP Network Service can be defined as default for H.323 connections and another Network Service as default for SIP connections. If the IP Network Service supports both H.323 and SIP connections, you can set the same Network Service as default for both H.323 and SIP, or for H.323-only or for SIP-only.

To designate an IP Network Service as the default IP Network Service:

- 1 In the Device Management pane, click IP Network Services (@).
- 2 In the **Network Services** list pane right-click the IP Network Service to be set as the default, and then click **Set As H.323 Default**, or **Set As SIP Default**.

The next time you access this menu, a check mark is added next to the network service type to indicate its selection as default.

To set this IP Network Service for both H.323 and SIP connections, repeat step 2 and select the option you need.

The following icons are used to indicate the default IP Network Service type:

Default IP Network Service Icons

Icon	Description			
45IP 2032	This Network Service supports both SIP and H.323 connections and is designated as default for both SIP and H.323 connections.			
≪SIP B23	This Network Service supports both SIP and H.323 connections and is designated as default for H.323 connections.			
(SIP 323/	This Network Service supports both SIP and H.323 connections and is designated as default for SIP connections.			
(B)	This Network Service supports only H.323 connections and is set as default for H.323 connections.			
SIP	This Network Service supports only SIP connections and is set as default for SIP connections.			

Ethernet Settings

The Collaboration Server is set to automatically identify the speed and transmit/receive mode of each LAN ports located on the RTM LAN or RTM ISDN cards that are added to the system. These port settings can be manually configured if the specific switch requires it, via the **Ethernet Settings** dialog box. For more details, see **Ethernet Settings**.



RealPresence Collaboration Server (RMX) 1500: The **Port** numbers displayed in the dialog box do not reflect the physical **Port** numbers as labeled on the RealPresence Collaboration Server (RMX) 1500 MCU.

Signaling Host IP Address and MCU Prefix in GK Indications

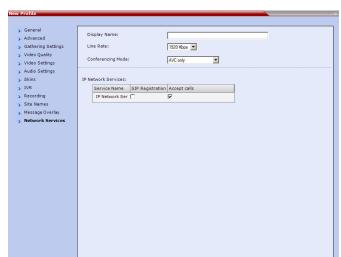
The Collaboration Server Web Client displays the Signaling Host IP Address and MCU Prefix in GK parameters as defined in the Default H.323 Network Service.

Video/Voice Port Configuration and Resolution Configuration (Collaboration Server 1500/2000/4000 in MPMx Card Configuration Mode only)

These configurations are set for the system and are applied to all the Network Services.

Conference Profile

Registration of conferencing entities such as ongoing conferences, Meeting Rooms, Entry Queues, SIP Factories and Gateway Sessions with SIP servers is done per conferencing entity. This allows better control on the number of entities that register with each SIP server by selecting for each of the conferencing entities whether it will register with the SIP server.



The registration is defined in the **Conference Profile - Network Services** tab.

In the **IP Network Services** table, the system lists all the defined Network Services (one or several depending on the system configuration).

- To register the conferencing entity to which this profile is assigned to a Network Service, in the **Registration** column click the check box of that Network Service.
- You can also prevent dial in participants from connecting to that conferencing entities when connecting via a Network Service.

In the **Accept Calls** column, clear the check box of the Network Service from which calls cannot connect to the conference.

Gateway Profiles

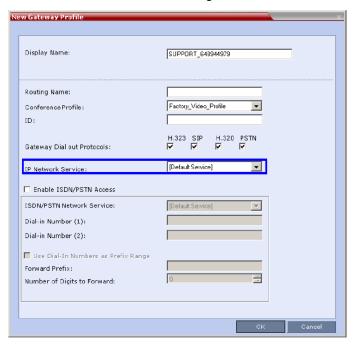


Gateway Services are not supported with the RealPresence Collaboration Server 1800.

To enable the Collaboration Server to call the destination endpoint/MCU via IP connection, the Network Service for the call must be selected in the Gateway Profile dialog box.

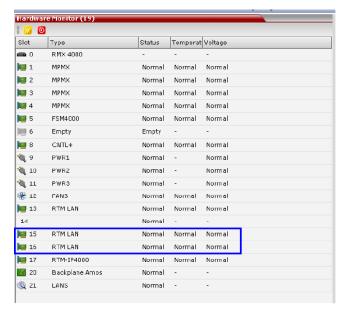
The Network Service set as default is used if no other Network Service is selected.

If the same Network Service is used for H.323 and SIP calls, the **Network Service Environment** must include both **H.323** and **SIP** settings.



Hardware Monitor

The Hardware Monitor pane includes the status of the LAN ports on the RTM LAN cards.



Signaling Monitor

The Signaling Monitor pane includes the list of the IP Network Services defined in the system (up to two in the RealPresence Collaboration Server (RMX) 1500/RealPresence Collaboration Server (RMX) 2000 and up to four in the RealPresence Collaboration Server (RMX) 4000). Double-clicking a Network Service, displays it properties and status.



Conferencing

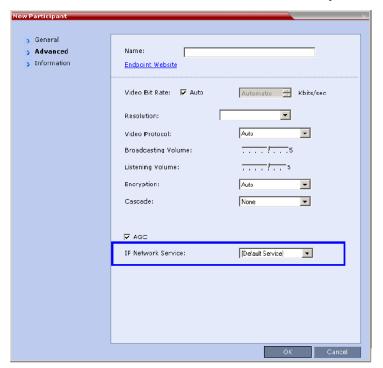
Each conference on the Collaboration Server can host participants from the different IP Network networks simultaneously.

Defining Dial Out Participants

When defining dial out participants, you can select the Network Service to place the call according to the network to which the endpoint pertains. If the endpoint is located on a network other than the selected network, the participant will not be able to connect.

If no Network is selected, the system uses the IP Network Service selected for reserving the conference resources, and if none is set for the conference it uses the Network Service set as default.

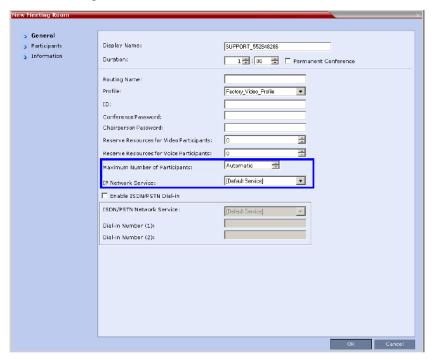
The IP Network Service is selected in the New Participant - Advanced dialog box.



Reserving Video Resources for a Conference (Collaboration Server 1500/2000/4000 only)

When defining a new ongoing conference or a conference reservation, you can select the Network Service that will be used to reserve the required resources. If no Network Service is selected, the default Network Service is used. Therefore, make sure that not all conferences are reserving resources from the same Network Service, otherwise you may run out of resources for that Network Service.

The IP Network Service is selected in the **New Conference/New Meeting Room/New Reservation - General** dialog box.



Monitoring Conferences

The Conference Properties - Network Services dialog box shows for each Network Service with which Network Service's SIP proxy the conference should be registered and if the dial in call will be connected to the conference.

In the Participant pane, a new column - Service Name was added, indicating the name of Network Service used for the participant's connection.

Resource Report

The Resource Report displays a graph of the MCU's total resource usage as well as a graph of the MCU's total resource usage. When Multiple Network Services are active, an additional table of resource usage per network service is displayed.

Video resource allocations are reported in AVC HD720p30 units. The same amounts of system resources are allocated to Voice (Audio) participants, as those allocated to CIF Video participants.

The user can select a view of either resource usage Totals (default) or resource usage per Network Service.

For Collaboration Servers 1500 and 2000/4000 with MPMx media cards both Video and Audio resource usage is displayed.

For Collaboration Servers 1800 and 2000/4000 with MPMRx media cards there is no differentiation between Video and Voice (Audio) resource usage.

Resource Report - Collaboration Servers 1500 and 2000/4000 with MPMx Cards



Show Graph Resources Graph Occupied Free Video Unit= Video (Occupied: 12%) Occupied Free Total Video Resources per Service Service Type / Occupied Free Total IP Network Se audio IP Network Se video 19 131 150 Service2 audio 0 Service2 video 150 150

Resource Report - Collaboration Servers 1800 and 2000/4000 with MPMRx Cards

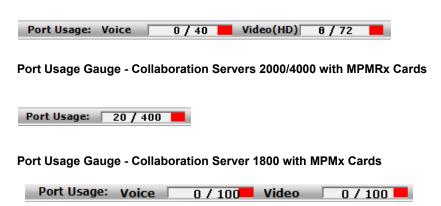
Port Usage Gauges

Collaboration Servers 1500 and 2000/4000 with MPMx media cards display port usage for Voice (Audio) and Video separately.

Collaboration Servers 1800 and 2000/4000 with MPMRx media cards do not differentiate between Video and Voice (Audio) resource usage and display a single port usage gauge.

The Port Gauge(s) show the total resource usage for the Collaboration Server and not per Network Service. So it may not be an accurate representation of the availability of resources for conferencing, as one Network Service may run out of available resources while another Network Service may have all of it resources available. In such a case, the port gauge(s) may show that half of the system resources are available for conferencing, while calls via the Network Service with no available resources will fail to connect.

Port Usage Gauges - Collaboration Servers 1500 and 2000/4000 with MPMx Cards



Port Usage Gauge - Collaboration Server 1800 with MPMRx Cards



NAT (Network Address Translation) Traversal

NAT Traversal is a set of techniques enabling participants behind firewalls to connect to conferences, hosted on the Collaboration Server, remotely using the internet.

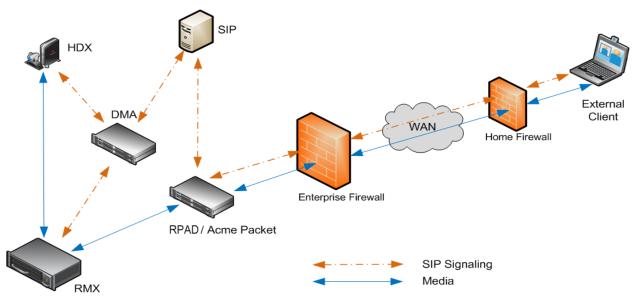
All signaling and media for both SIP and H.323 will be routed through an **SBC**. The following **SBC** environments are supported:

- SAM a Polycom SBC
- Acme Packet a 3rd party SBC
- VBP Polycom Video Border Proxy

Deployment Architectures

The following NAT Traversal topologies are given as examples. Actual deployments will depend on user requirements and available infrastructure:

Remote Connection Using the Internet



The following **Remote Connection** call flow options are supported:

Remote Connections

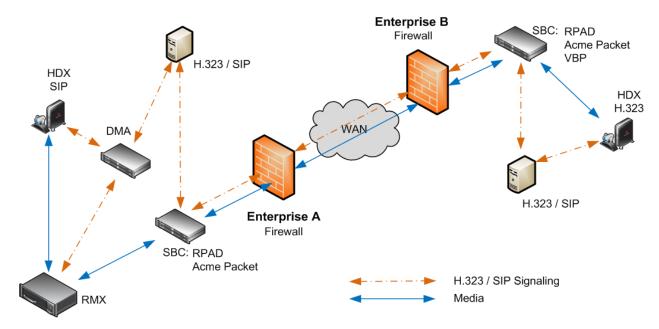
Enterprise Client				CMA Client	
Environment	Registered	SBC		Registered	Environment
SIP / H.323	Yes	SAM / Acme Packet	⇔	Yes	SIP

Remote Connections

Enterprise Client			
Environment	Registered	SBC	
SIP / H.323	No	SAM / Acme Packet	⇔
SIP / H.323	No	SAM Only	⇔

CMA Client	
Registered	Environment
No	SIP
No	H.323

Business to Business Connections



The following **Business to Business** connection call flow options are supported:

Business to Business Connections

Enterprise A Client			
Environment	Registered	SBC	
H.323	Yes	RPAD	
H.323	Yes	RPAD	=
SIP	Yes	RPAD	=
SIP	Yes	Acme Packet	←

Enterprise B Client		
SBC	Registered	Environment
RPAD	Yes	H.323
VBP	Yes	H.323
RPAD	Yes	H.323
Acme Packet	Yes	H.323

FW (Firewall) NAT Keep Alive

The Collaboration Server can be configured to send a FW NAT keep alive message at specific Intervals for the RTP, UDP and BFCP channels.

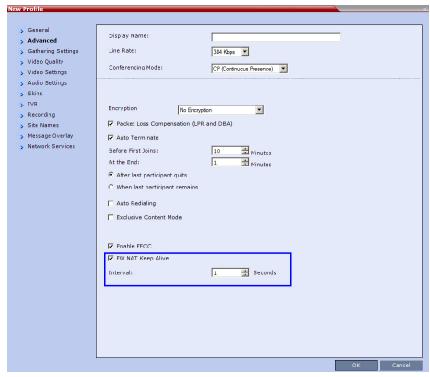
This is necessary because port mappings in the firewall are kept open only if there is network traffic in both directions. The firewall will only allow UDP packets into the network through ports that have been used to send packets out.

By default the Collaboration Server sends a FW NAT Keep Alive message every 30 seconds. As there is no traffic on the Content and FECC channels as a call begins, the firewall will not allow any incoming packets from the Content and FECC channels in until the Collaboration Server sends out the first of the FW NAT Keep Alive messages 30 seconds after the call starts.

If Content or FECC are required within the first 30 seconds of a call the **FW NAT Keep Alive Interval** should be modified to a lower value.

To enable and modify FW NAT Keep Alive:

FW NAT Keep Alive is enabled in the New Profile - Advanced dialog box.



» Select the FW NAT Keep Alive check box and if required, modify the Interval field within the range of 5 - 86400 seconds.

System Configuration in SBC environments

In an environment that includes SAM (a Polycom SBC), to ensure that a RealPresence Mobile endpoint can send content to a conference the value of the system flag

NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT must be set to at least 3.

For more details on modifying the values of system flags, see Modifying System Flags.

SIP TCP Keep-Alive

SIP TCP Keep Alive behavior is defined for each IP Network Service and can be modified by adding the following System Flags and modifying their values:

- SIP_TCP_KEEPALIVE_TYPE
- SIP_TCP_KEEP_ALIVE_BEHAVIOR

For a detailed description see SIP TCP Keep-Alive.

IVR Services

Interactive Voice Response (IVR) is an application that allows participants to communicate with the conferencing system via their endpoint's input device (such as a remote control). The IVR Service includes a set of voice prompts and a video slide used to automate the participants connection to a conference or Entry Queue. It allows customization of menu driven scripts and voice prompts to meet different needs and languages.

The IVR module includes two types of services:

- Conference IVR Service that is used with conferences
- Entry Queue IVR Service that is used with Entry Queues

The system is shipped with two default Conference IVR Services (one for the conferences and the other for gateway calls) and one default Entry Queue IVR Service. The default services include voice messages and video slides in English.

To customize the IVR messages and video slide perform the following operations:

- Record the required voice messages and create a new video slide.
 For more information, see Creating a Welcome Video Slide.
- Optional. Add the language to the list of languages supported by the system.
- Upload the voice messages to the MCU (This can be done as part of the language definition or during the IVR Service definition).
- Create the Conference IVR Service and upload the video slide, and if required any additional voice messages.
- Optional. Create the Entry Queue IVR Service and upload the required video slide and voice messages.



When upgrading the *Collaboration Server* software version new DTMF Codes and voice messages are not automatically added to existing IVR Services in order to avoid conflicts with existing DTMF codes. Therefore, to use new options, new Conference and Entry Queue IVR Services must be created.

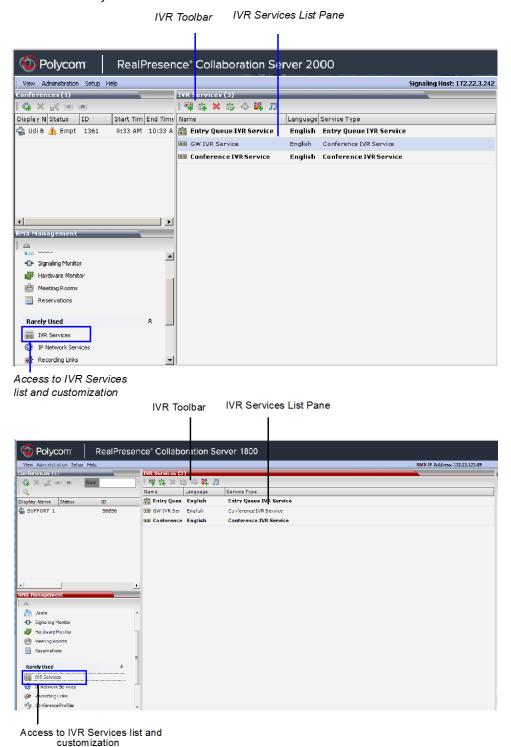
IVR Services List

You can view the currently defined Conference IVR and Entry Queue IVR Services in the **IVR Services** list pane.

To view the IVR Services list:

- 1 In the Collaboration Server Management pane, expand the Rarely Used list.
- 2 Click the IVR Services (em) entry.

The list pane displays the Conference IVR Services list and the total number of IVR services currently defined in the system.



IVR Services Toolbar

The IVR Services toolbar provides quick access to the IVR Service definitions as follows:

IVR Toolbar buttons

Button	Button Name	Descriptions
#5	New Conference IVR Service	To create a new Conference IVR Service.
֠+	New Entry Queue IVR Service	To create a new Entry Queue IVR Service.
*	Delete Service	Deletes the selected IVR service(s).
	Set Default Conference IVR Service	Sets the selected Conference IVR Service as default. When creating a new conference Profile the default IVR Service is automatically selected for the Profile (but can be modified).
4	Set Default Entry Queue Service	Sets the selected Entry Queue IVR Service as default. When creating a new Entry Queue the default Entry Queue IVR Service is automatically selected.
犇	Add Supported Languages	Adds languages to the IVR module, enabling you to download voice prompts and messages for various languages.
IJ	Replace/Change Music File	To replace the currently loaded music file that is used to play background music, the MCU is shipped with a default music file.

Adding Languages

You can define different sets of audio prompts in different languages, allowing the participants to hear the messages in their preferred language.

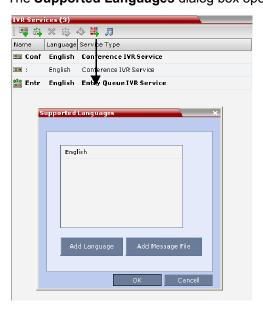
The Collaboration Server is shipped with a default language (English) and all the prompts and messages required for the default IVR Services, conference and Entry Queues shipped with the system.

You can add languages to the list of languages for which different messages are downloaded to the MCU and IVR Services are created. This step is required before the creation of additional IVR messages using languages that are different from English, or if you want to download additional voice files to existing files in one operation and not during the IVR service definition.

To add a language:

- 1 In the Collaboration Server Management pane, expand the Rarely Used list.
- 2 Click the IVR Services (em) entry.

3 In the Conference IVR Services list, click the **Add Supported Languages** (■) button. The **Supported Languages** dialog box opens.



4 Click the Add Language button.

The New Language dialog box opens.



- 5 In the **New Language** dialog box, enter the name of the new language. The language name can be typed in Unicode and cannot start with a digit. Maximum field length is 31 characters.
- Click OK.

The new language is added to the list of Supported Languages.

Uploading a Message File to the Collaboration Server

You can upload audio files for the new language or additional files for an existing language now, or you can do it during the definition of the IVR Service. In the latter case, you can skip the next steps.



- Voice messages should not exceed 3 minutes.
- It is not recommended to upload more than 1000 audio files to the MCU memory.

To upload messages to the MCU:

1 To upload the files to the MCU, in the Supported Languages dialog box, click the Add Message File button.

The Add Message File dialog box opens.



Audio files are uploaded to the MCU one-by-one.

- 2 In the IVR Message Language list, select the language for which the audio file will be uploaded to the MCU.
- 3 In the IVR Message Category list, select the category for which the audio file is uploaded.
- In the Message Type list, select the message type for which the uploaded message is to be played. You can upload several audio files for each Message Type. Each file is downloaded separately.
 Table 5-2 lists the Message Types for each category:

IVR Message Types by Message Category

Message Category	Message Type	Message
Conference Password	Request Conference Password	Requests the participant to enter the conference password.
	Request Conference Password Retry	A participant who enters an incorrect password is requested to enter it again.
	Request Digit	Requests the participant to enter any digit in order to connect to the conference. Used for dial-out participants to avoid answering machines in the conference.
Welcome Message	Welcome Message	The first message played when the participant connects to the conference or Entry Queue.
Conference Chairperson	Request Chairperson Identifier	Requests the participants to enter the chairperson identifier key.
	Request Chairperson Password	Requests the participant to enter the chairperson password.
	Request Chairperson Password Retry	When the participant enters an incorrect chairperson password, requests the participant to enter it again.

IVR Message Types by Message Category

Message Category	Message Type Message	
General	Messages played for system related event notification conference is locked. Upload the files for the voice nevent occurs during the conference. For more inform Properties - General Voice Messages.	nessages that are played when an
Billing Code	Requests the chairperson to enter the conference Bi	lling Code.
Roll Call	Roll call related messages, such as the message pla conference. Messages are listed in the Conference I	
Conference ID	Requests the participant to enter the required Confe destination conference.	rence ID to be routed to the

5 Click **Upload File** to upload the appropriate audio file to the MCU.

The Install File dialog box opens.



6 Enter the file name or click the **Browse** button to select the audio file to upload.

The Select Source File dialog box opens.

- 7 Select the appropriate *.wav audio file, and then click the Open button.
 The name of the selected file is displayed in the Install field in the Install File dialog box.
- 8 Optional. You can play a .wav file by selecting the **Play** button (2).
- **9** Click Yes to upload the file to the MCU.

The system returns to the **Add Message File** dialog box.

- 10 Repeat step 6 for each additional audio file to be uploaded to the MCU.
- 11 Once all the audio files are uploaded to the MCU, close the **Add Message File** dialog box and return to the **Add Language** dialog box.
- 12 Click OK.

Defining a New Conference IVR Service

The Collaboration Server is shipped with two default Conference IVR Services and all its audio messages and video slide. You can define new Conference IVR Services or modify the default Conference IVR Service. For the definition of Conference IVR Service for gateway calls, see Defining the IVR Service for Gateway Calls.

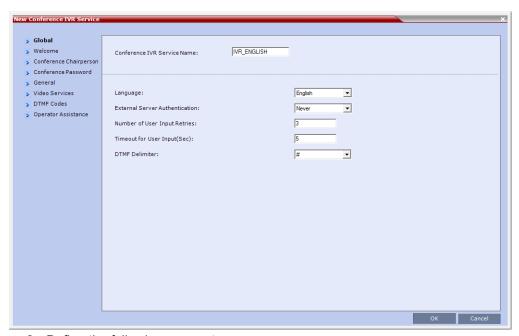


Up to 80 IVR Services (Conference IVR Services and Entry Queue IVR Services) can be defined per Collaboration Server.

Defining a New Conference IVR Service

To define a new Conference IVR Service:

1 On the IVR Services toolbar, click the New Conference IVR Service () button. The New Conference IVR Service - Global dialog box opens.



2 Define the following parameters:

Conference IVR Service Properties - Global Parameters

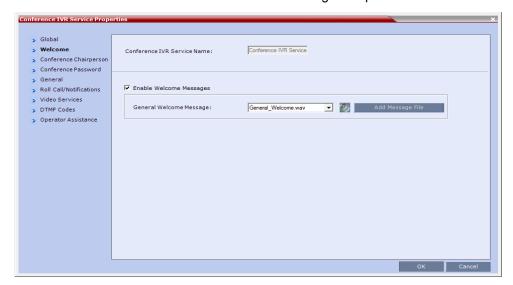
Field/Option	Description
Conference IVR Service Name	Enter the name of the Conference IVR Service. The maximum field length is 20 characters and may be typed in Unicode.
Language For IVR	Select the language of the audio messages and prompts from the list of languages defined in the Supported languages. The default language is English. For more information, see Adding Languages.

Conference IVR Service Properties - Global Parameters

Field/Option	Description
External Server Authentication	 This option is not supported with Collaboration Server 1800. You can configure the IVR Service to use an external database application to verify a participant's right to join the conference. For more information, see Conference Access with External Database Authentication. Select one of the following options: Never – The participant's right to join the conference will not be verified with an external database application (default). Always – Any participant request to join the conference is validated with the external database application using a password. Upon Request – Only the participant request to join the conference as chairperson is validated with the external database application using a password. The validation process occurs only when the participant enters the chairperson identifier key.
Number of User Input Retries	Enter the number of times the participant will be able to respond to each menu prompt before being disconnected from the conference. Range is between 1-4, and the default is 3.
Timeout for User Input (Sec)	Enter the duration in seconds that the system will wait for the participant's input before prompting for another input. Range is between 1-10, and the default value is 5 seconds.
DTMF Delimiter	Enter the key that indicates the last input key. Possible values are the pound (#) and star (*) keys. The default is #.

3 Click the Welcome tab.

The New Conference IVR Service - Welcome dialog box opens.



- 4 Select the **Enable Welcome Messages** check box to define the system behavior when the participant enters the Conference IVR queue. When participants access a conference through an Entry Queue, they hear messages included in both the Entry Queue Service and Conference IVR Service. To avoid playing the Welcome Message twice, disable the Welcome Message in the Conference IVR Service.
- 5 Select the **General Welcome Message**, to be played when the participant enters the conference IVR queue.
- 6 To upload an audio file for an IVR message, click Add Message File.

The Install File dialog box opens.

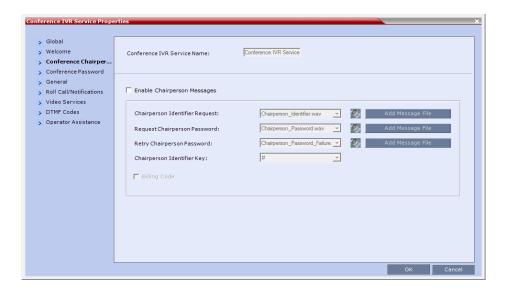




The Collaboration Server unit is bundled with default audio IVR message files. To upload a customized audio file, see Creating Audio Prompts and Video Slides.

- a Click the Browse button to select the audio file (*.wav) to upload.
 - The **Select Source File** dialog box opens.
- **b** Select the appropriate *.wav audio file and then click the **Open** button.
- **c** Optional. You can play a .wav file by selecting the **Play** button (**9**).
- d In the Install File dialog box, click Yes to upload the file to the MCU memory.
 - The **Done** dialog box opens.
- **e** Once the upload is complete, click **OK** and return to the IVR dialog box. The new audio file can now be selected from the list of audio messages.
- 7 Click the Conference Chairperson tab.

The New Conference IVR Service - Conference Chairperson dialog box opens.



8 Select the **Enable Chairperson Messages** check box to enable the chairperson functionality. If this feature is disabled, participants are not able to connect as the chairperson.



When both Conference Password and Chairperson Password options are enabled and defined, the system first plays the prompt Enter conference password. However, if the participant enters the chairperson password, the participant becomes the chairperson.

To play the prompt requesting the Chairperson password, For conference chairperson services..., do not select the Enable Password Messages option.

9 Select the various voice messages and options for the chairperson connection.



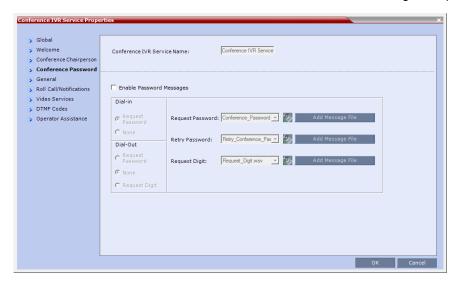
If the files were not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the Collaboration Server.

New Conference IVR Service Properties - Conference Chairperson Options and Messages

Field/Option	Description
Chairperson Identifier Request	Select the audio file that requests the participants to enter the key that identifies them as the conference chairperson.
Request Chairperson Password	Select the audio file that prompts the participant for the chairperson password.
Retry Chairperson Password	Select the audio file that prompts participants to re-enter the chairperson password if they enter it incorrectly.
Chairperson Identifier Key	Enter the key to be used for identifying the participant as a chairperson. Possible keys are: pound key (#) or star (*).
Billing Code	The prompt requesting the chairperson billing code selected in the General tab.

10 Click the Conference Password tab.

The New Conference IVR Service - Conference Password dialog box opens.



11 Select the **Enable Password Messages** check box to request the conference password before moving the participant from the conference IVR queue to the conference.



When both Conference Password and Chairperson Password are enabled and defined, the system first plays the prompt Enter conference password. However, if the participant enters the chairperson password, the participant becomes the chairperson.

To play the prompt requesting the Chairperson password, For conference chairperson services..., do not select the **Enable Password Messages** option.

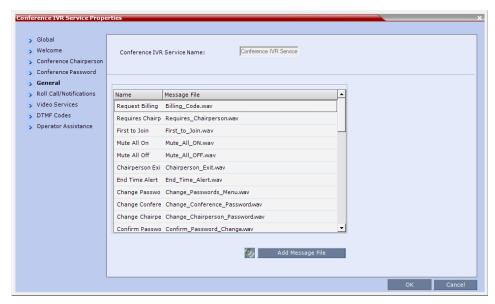
- **12** Select the MCU behavior for password request for Dial-in and Dial-out participant connections. Select the required system behavior as follows:
 - Request password The system requests the participant to enter the conference password.
 - None The participant is moved to the conference without any password request.
 - Request Digit The system requests the participant to enter any key. This option is used mainly for dial-out participants and to prevent an answering machine from entering the conference.
- 13 Select the various audio messages that will be played in each case.

New Conference IVR Service Properties - Conference Password Parameters

Option	Description
Request Password	Select the audio file that prompts the participant for the conference password.
Retry Password	Select the audio file that requests the participant to enter the conference password again when failing to enter the correct password.
Request Digit	Select the audio file that prompts the participant to press any key when the Request Digit option is selected.

14 Click the General tab.

The New Conference IVR Service - General dialog box opens.



The **General** dialog box lists messages that are played during the conference. These messages are played when participants or the conference chairperson perform various operations or when a change occurs.

- **15** To assign the appropriate audio file to the message type, click the appropriate table entry, in the **Message File** column. A drop-down list is enabled.
- **16** From the list, select the audio file to be assigned to the event/indication.
- **17** Repeat steps 15 and 16 to select the audio files for the required messages.

The following types of messages and prompts can be enabled:

Conference IVR Service Properties - General Voice Messages

Message Type	Description
Blip on Cascade Link	Indicates that the link to the cascaded conference connected successfully.
Chairperson Exit	Informs all the conference participants that the chairperson has left the conference, causing the conference to automatically terminate after a short interval. Note: This message is played only when the Requires Chairperson option is selected in the Conference Profile - IVR dialog box.
Chairperson Help Menu	A voice menu is played upon a request from the chairperson, listing the operations and their respective DTMF codes that can be performed by the chairperson. The playback can be stopped any time.
	Note: If you modify the default DTMF codes used to perform various operations, the default voice files for the help menus must be replaced.
Change Chairperson Password	Requests the participant to enter a new chairperson password when the participant is attempting to modify the chairperson password.

Conference IVR Service Properties - General Voice Messages

Message Type	Description	
Change Conference Password	Requests the participant to enter a new conference password when the participant is attempting to modify the conference password.	
Change Password Failure	A message played when the participant enters an invalid password, for example when a password is already in use.	
Change Passwords Menu	This voice menu is played when the participants requests to change the conference password. This message details the steps required to complete the procedure.	
Conference is Locked	This message is played to participants attempting to join a Secured conference.	
Conference is Secured	This message is played when the conference status changes to Secure as initiated by the conference chairperson or participant (using DTMF code *71).	
Conference is unsecured	This message is played when the conference status changes to Unsecured as initiated by the conference chairperson or participant (using DTMF code #71).	
Confirm Password Change	Requests the participant to re-enter the new password.	
Dial Tone	The tone that will be played to indicate a dialing tone, to let the calling participant enter the destination number. Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.	
Disconnect on Busy	The Busy Tone is played when the system retries to redial a busy destination number and fails after exceeding the number of redials. This call is then disconnected. Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.	
Disconnect on No Answer	The Reorder Tone is played when the system retries to redial a destination number that does not answer and fails after exceeding the number of redials. This call is then disconnected. Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.	
Disconnect on Wrong Number	ct on Wrong A voice message is played when the call fails because of an incorrect destination number. The message is followed the Reorder Tone and the call is disconnected. Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.	
End Time Alert	Indicates that the conference is about to end.	
Enter Destination ID	Prompts the calling participant for the destination number. Default message prompts the participant for the conference ID (same message as in the Entry Queue IVR Service).	
	Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.	
First to Join	Informs the participant that he or she is the first person to join the conference.	

Conference IVR Service Properties - General Voice Messages

Message Type	Description	
Incorrect Destination ID	If the participant entered an incorrect conference ID (in gateway calls it is the destination number), requests the participant to enter the number again. Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.	
Maximum Number of Participants Exceeded	Indicates the participant cannot join the destination conference as the maximum allowed number of participants will be exceeded.	
Mute All Off	This message is played to the conference to inform all participants that they are unmuted (when Mute All is cancelled).	
Mute All On	Informs all participants that they are muted, with the exception of the conference chairperson. Note: This message is played only when the Mute All Except Me option is activated.	
No Video Resources Audio Only.	Informs the participant of the lack of Video Resources in the <i>Collaboration Server</i> and that he/she is being connected as Audio Only.	
Participant Help Menu	A voice menu that is played upon request from a participant, listing the operations and their DTMF codes that can be performed by any participant.	
Password Changed Successfully	A message is played when the password was successfully changed.	
Recording Failed	This message is played when the conference recording initiated by the chairperson or the participant (depending on the configuration) fails to start.	
Recording in Progress	This message is played to participant joining a conference that is being recorded indicating the recording status of the conference.	
Redial on Wrong Number	A message is played requesting the participant to enter a new destination number followed by up to five redial attempts. If all redial attempts fail, the participant is alerted by an IVR message that the dialed number is unreachable, followed by the Reorder Tone and disconnection. Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.	
Request Billing Code	Requests the participant to enter a code for billing purposes.	
Requires Chairperson	The message is played when the conference is on hold and the chairperson joins the conference. For this message to be played the Conference Requires Chairperson option must be selected in the Conference Profile - IVR dialog box.	
Ringing Tone	The tone that will be played to indicate that the system is calling the destination number. Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.	
Self Mute	A confirmation message that is played when participants request to mute their line.	

Conference IVR Service Properties - General Voice Messages

Message Type	Description
Self Unmute	A confirmation message that is played when participants request to unmute their line.

18 Click the Roll Call/Notifications tab.

The New Conference IVR Service - Roll Call dialog box opens.



The Roll Call and Tone Notification options are disabled in SVC and mixed CP and SVC conferences.

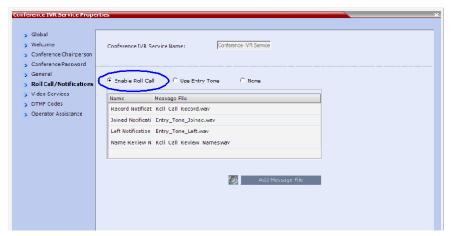
The **Roll Call** feature of the Conference IVR Service is used to record the participants' names for playback when the participants join and leave a conference.

Roll Call announcements played upon a participant's connection or disconnection from a conference (Entry and Exit announcements) can be replaced by tones. These tones can be used as notification when participants join or leave the conference but the identification of the participant is not required. The system is shipped with two default tones: **Entry Tone** and **Exit tone**. When the Tone Notifications option is enabled, no recording of the participant names will occur and the conference chairperson will not be able to ask for a name review during the conference.

In Collaboration Server 1500/2000/4000, from version 7.6 the selection of tones in the IVR Service definition replaces the functionality of the system flag

IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE.

- **19** Select one of the following options to determine the announcement mode:
 - a To enable the Roll Call feature, select the **Enable Roll Call** option.



b Select Enable Tones to enable the Tone Notifications option.

The dialog box changes to display the tone notification options and all Roll Call options are disabled. In such a case, skip to step.

c Select None to disable the Roll Call and Tone Notifications features.

20 If Enable Roll Call option is selected: To assign the audio file to the message type, in the Message File column, click the appropriate table entry.

An arrow appears in the **Message File** column.



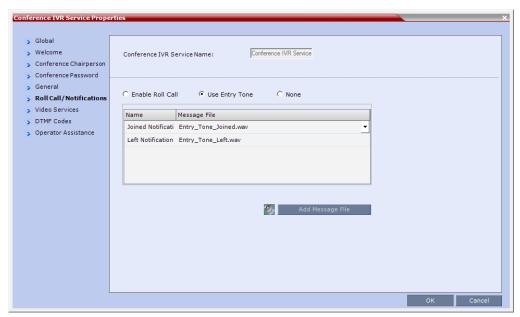
If the Roll Call option is enabled, you must assign the appropriate audio files to all message types.

21 Click the arrow to open the Message File list and select the appropriate audio file.

Conference IVR Service Properties - Roll Call Messages

Roll Call Message	Description	
Roll Call Record	Requests participants to state their name for recording, when they connect to the conference. Note: The recording is automatically terminated after two seconds.	
	Note. The recording is automatically terminated after two seconds.	
Roll Call Joined	A voice message stating that the participant has joined the conference. Note: In Collaboration Server 1500/2000/4000, in versions prior to 7.6, when the system flag IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE is set to YES, the system does not playback the Roll Call names when participants enter the conference. However, the voice message will be played, unless it is replaced with tone file. In such a case, the use of tones requires the uploading of the appropriate tone files in *.wav format and replacing the Roll Call Joined message file with the tone file.	
Roll Call Left	A voice message stating that the participant has left the conference. Note: In Collaboration Server 1500/2000/4000, from version 7.6, in versions prior to 7.6, when the system flag IVR_ROLL_CALL_USE_TONES_INSTEAD_OF_VOICE is set to YES, the system does not playback the Roll Call names when participants exit the conference. However, the voice message will be played, unless it is replaced with tone file. In such a case, the use of tones requires the uploading of the appropriate tone files in *.wav format and replacing the Roll Call Left message file with the tone file.	
Roll Call Review	Played when Roll Call is requested by the chairperson, introducing the names of the conference participants in the order they joined the conference.	

22 If Enable Tone Notifications option is selected: Select the Entry Tone or Exit tone:



- a Click the appropriate table entry in the Message File column.
 A drop-down list is enabled.
- **b** From the list, select the audio file to be assigned to the event/indication.



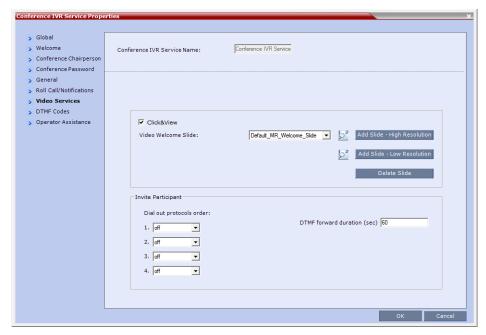
If the **Tones** option is enabled, you must assign the appropriate audio files to all notification types. The Collaboration Server system is shipped with two default tones: **Entry_tone.wav** and **Exit_tone.wav**.

If required, you can upload customized audio files that will be played when participants join or leave the conference.

If the option to play a tone when a cascading link connection is established, make sure that the tone selected for Entry or Exit notification differ from the cascading link tone as the latter one cannot be customized.

23 Click the Video Services tab.

The New Conference IVR Service - Video Services dialog box opens.





The Click&View and Invite Participants features are disabled in SVC and mixed CP and SVC conferences.

In addition to the low and high resolution slides included in the default slide set, customized low and high resolution slides are supported.

The following guidelines apply:

- > Two customized slides can be loaded per IVR Service:
 - ♦ A low resolution slide, to be used with low resolution endpoints.
 - ♦ A high resolution slide, to be used with high resolution endpoints.

The following table summarizes the recommended input slide formats and the resulting slides that are generated:

IVR Slide - Input / Output Formats

	Format	Format	
Slide Resolution	Input Slides	Generated Slides	
	HD1080p (16:9)	HD1080p	
	or	HD720p	
High	HD720p (16:9)		

IVR Slide - Input / Output Formats

	Format	Format	
Slide Resolution	Input Slides	Generated Slides	
	4CIF (4:3)	4SIF	
	or	SIF	
Low	CIF (4:3)	CIF	

- > The source images for the high resolution slides must be in *.bmp or *.jpg format.
- ➢ If the uploaded slides are not of the exact SD or HD resolution, an error message is displayed and the slides are automatically cropped or enlarged to the right size.
- If a slide that is selected in an IVR Service is deleted, a warning is displayed listing the IVR Services in which it is selected. If deleted, it will be replaced with a default Collaboration Server slide.
- > The generated slides are not deleted if the system is downgraded to a lower software version.
- The first custom source file uploaded, whatever its format, is used to generate both high and low resolution custom slides. High resolution source files uploaded after the first upload will be used to generate and replace high resolution custom slides. Likewise, low resolution source files uploaded after the first upload will be used to generate and replace low resolution custom slides.
- ➤ If there are two custom source files in the folder, one high resolution, one low resolution, and a new high resolution custom source file is uploaded, new high resolution custom slides are created. The existing low resolution custom slides are not deleted.
- ➤ If there are two custom source files in the folder, one high resolution, one low resolution, and a new low resolution custom source file is uploaded, new low resolution custom slides are created. The existing high resolution custom slides are not deleted.

24 Define the following parameters

New Conference IVR Service Properties - Video Services Parameters

Video Services	Description
Click&View	Select this option to enable endpoints to run the Click&View application that enables participants to select a video layout from their endpoint. Note: This option is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.
Video Welcome Slide	Select the Low Resolution and High Resolution video slides to be displayed when participants connect to the conference. To view any slide, click the Preview Slide () button. Notes: When using one of the default Polycom slides, the slide will be displayed in the resolution defined in the profile, i.e. CIF, SD, HD 720p or HD 1080p. When defining a gateway IVR Service, the recommended default slide is: Default_GW_Welcome_Slide. Customized H.261 slides are not supported. When Collaboration Server is configured to IPv6, the IVR slide is displayed without taking into account the MTU Size.

New Conference IVR Service Properties - Video Services Parameters

Video Services	Description
Invite Participant	See Inviting Participants using DTMF. Note: The Invite Participant feature is not available in SVC conferences and for SVC participants in mixed CP and SVC conferences.
Dial out protocols order	Select the order of the network protocols that will be used by the system to dial the destination number. The system will start dialing using the first protocol, and if the call is not answered it will continue with the second, third and fourth protocols (if they are enabled) until the call is answered. By default, H.323 is set as the first protocol and SIP as the second while the remaining protocols are disabled (set to Off). For PSTN calls, select the PSTN protocol and not ISDN. Set PSTN before ISDN if both PSTN and ISDN protocols are required.
DTMF forward duration	Use this field when connecting to another conferencing entity with an IVR, requiring the input of a password, destination number or ID. Enter the number of seconds that the system will wait for the input of additional DTMF digits such as a password or conference number. Range: 10 - 600 seconds Default: 60 seconds.

25 If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click the:

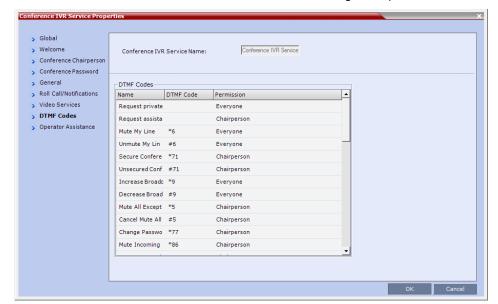
- > Add Slide Low Resolution button to upload a Low Resolution Slide.
- > Add Slide High Resolution button to upload a High Resolution Slide.

The **Install File** dialog box opens. The uploading process is similar to the uploading of audio files. For more information, see step 6 above.



- The video slide must be in a .jpg or .bmp file format. For more information, see Creating a Welcome Video Slide.
- Customized H.261 slides are not supported.

26 Click the DTMF Codes tab.



The New Conference IVR Service - DTMF Codes dialog box opens.

 This dialog box lists the default DTMF codes for the various functions that can be performed during the conference by all participants or by the chairperson

New Conference IVR Service Properties - DTMF Codes

Operation	DTMF String	Permission
Mute My Line	*6	Everyone
Unmute My Line	#6	Everyone
Increase Broadcast Volume Note: This option is not available for SVC participants.	*9	Everyone
Decrease Broadcast Volume Note: This option is not available for SVC participants.	#9	Everyone
Mute All Except Me	*5	Chairperson
Cancel Mute All Except Me	#5	Chairperson
Change Password	*77	Chairperson
Mute Incoming Participants	*86	Chairperson
Unmute Incoming Participants	#86	Chairperson
Play Help Menu	*83	Everyone
Enable Roll Call Note: This option is not available in SVC conferences.	*42	Chairperson
Disable Roll Call Note: This option is not available in SVC conferences.	#42	Chairperson

New Conference IVR Service Properties - DTMF Codes

Operation	DTMF String	Permission
Roll Call Review Names Note: This option is not available in SVC conferences.	*43	Chairperson
Roll Call Stop Review Names Note: This option is not available in SVC conferences.	#43	Chairperson
Terminate Conference	*87	Chairperson
Start Click&View Note: This option is not available for SVC participants.	**	Everyone
Start PCM Note: This option is not available for SVC participants.	##	Chairperson
Invite Participant Note: This option is not available for SVC participants.	*72	Everyone
Disconnect Last Invited Participant Note: This option is not available for SVC participants.	#72	Chairperson
Change To Chairperson	*78	Everyone
Increase Listening Volume Note: This option is not available for SVC participants.	*76	Everyone
Decrease Listening Volume Note: This option is not available for SVC participants.	#76	Everyone
Override Mute All	Configurable	Everyone
Start Recording	*3	Chairperson
Stop Recording	*2	Chairperson
Pause Recording	*1	Chairperson
Secure Conference	*71	Chairperson
Unsecured Conference	#71	Chairperson
Show Number of Participants Note: This option is not available in SVC conferences.	*88	Everyone
Request individual assistance Note: This option is not available for SVC participants.	*0	Everyone
Request assistance for conference Note: This option is not available for SVC participants.	00	Chairperson
Request to Speak	99	Everyone
Touch Control Prefix Note: This option is not available for SVC participants.	*#	Everyone



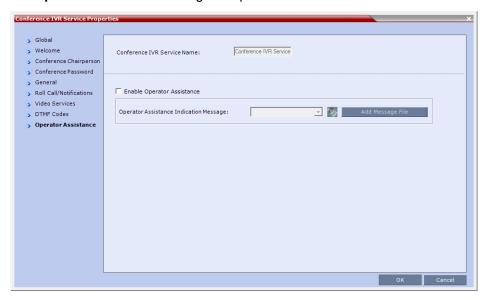
- Do not change the DTMF code of the Touch Control Prefix (*#).
 The Polycom® Touch Control device is only supported with MPM+ and MPMx media cards.
 For more information see the Polycom® Touch Control User Guide.
- If during the ongoing conference the Show Number of Participants DTMF option (default DTMF *88) is used, when the displayed number of participants is removed, the message overlay text is also removed.
- 27 To modify the DTMF code or permission:
 - a In the **DTMF Code** column, in the appropriate entry enter the new code.
 - **b** In the **Permission** column, select from the list who can use this feature (Everyone or just the Chairperson).



By default, the Secure, Unsecure Conference and Show Number of Participants options are enabled in the Conference IVR Service. These options can be disabled by removing their codes from the Conference IVR Service.

- To disable the Text Indication option in the DTMF Code column, clear the DTMF code (*88) of Show Number of Participants from the table.
- To disable the Secure Conference options, in the **DTMF Code** column, clear the DTMF codes of both Secured Conference (*71) and Unsecured Conference (#71) from the table.
- 28 Click the Operator Assistance tab.

The Operator Assistance dialog box opens.



29 Select Enable Operator Assistance to enable operator assistance when the participant requires or requests help during the connection process to the conference or during the conference.



The Operator Assistance option is disabled in SVC conferences.

30 In the Operator Assistance Indication Message field, select the audio message to be played when the participant requests or is waiting for the operator's assistance.



If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the Collaboration Server.

31 Click **OK** to complete the IVR Service definition.

The new Conference IVR Service is added to the IVR Services list.

Change to Chairperson

Regular participants can request to become the conference chairperson using the appropriate DTMF code (default: *78), which enabled them to perform operations designated for chairpersons only.

The Change to Chairperson via the DTMF code (default: *78) is executed only if the following settings were configured for the MCU and the conference:

- In the Conference IVR Service Conference Chairperson dialog box, select the Enable Chairperson Messages check box, and select the appropriate voice messages.
 - For more information, see New Conference IVR Service Properties Conference Chairperson Options and Messages.
- When starting a new conference or defining a new Meeting Room, define the Chairperson Password in the conference General dialog box.

For more information, see Creating a New Meeting Room.

Controlling the receipt of in-band and out-of-band DTMF Codes

The RFC2833_DTMF System Flag controls the receipt of in-band or out-of-band DTMF Codes.

When set to **YES** (default), the RMX will receive DTMF Codes sent in-band. When set to **NO** the RMX receives DTMF Codes sent out-of-band. The RMX always sends DTMF Codes in-band (as part of the Audio Media stream). If you wish to modify the flag value, the flag must be added to the System Configuration file. For more information see Modifying System Flags.

Entry Queue IVR Service

An Entry Queue (EQ) is a routing lobby for conferences. Participants are routed to the appropriate conference according to the conference ID they enter.

An Entry Queue IVR Service must be assigned to the Entry Queue to enable the voice prompts and video slide guiding the participants through the connection process.

An Entry Queue IVR Service is a subset of an IVR Service. You can create different Entry Queue Services for different languages and personalized voice messages.

The Collaboration Server is shipped with a default Entry Queue IVR Service and all its audio messages and video slide. You can define new Entry Queue IVR Services or modify the default Entry Queue IVR Service.

Defining a New Entry Queue IVR Service

To set up a new Entry Queue IVR Service:

- 1 In the RMX Management pane, click IVR Services ().
- 2 In the IVR Services list, click the New Entry Queue IVR Service () button.
 The New Entry Queue IVR Service Global dialog box opens.



3 Fill in the following parameters:

Entry Queue IVR Service Properties - Global Parameters

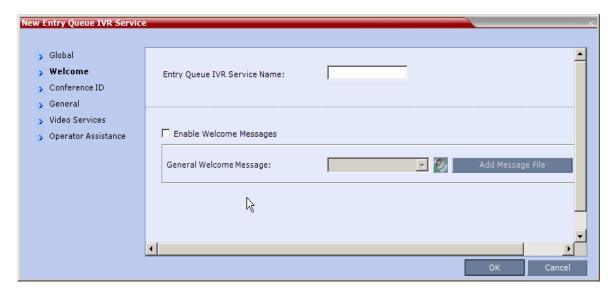
Option	Description	
Entry Queue Service Name	(Mandatory) Enter the name of the Entry Queue Service. The name can be typed in Unicode. Maximum field length is 80 ASCII characters.	
Language	Select the language in which the Audio Messages and prompts will be heard. The languages are defined in the Supported Languages function.	
External Server Authentication	 This option is used for Ad Hoc conferencing, to verify the participant's permission to initiate a new conference. For a detailed description see Appendix D - Ad Hoc Conferencing and External Database Authentication. Select one of the following options: None to start a new conference without verifying with an external database the user right to start it. Conference ID to verify the user's right to start a new conference with an external database application using the conference ID. 	
Number of User Input Retries	Enter the number of times the participant is able to respond to each menu prompt before the participant is disconnected from the MCU.	
Timeout for User Input (Sec.)	Enter the duration in seconds that the system waits for input from the participant before it is considered as an input error.	

Entry Queue IVR Service Properties - Global Parameters

Option	Description
DTMF Delimiter	The interaction between the caller and the system is done via touch-tone signals (DTMF codes). Enter the key that will be used to indicate a DTMF command sent by the participant or the conference chairperson. Possible keys are the pound key (#) or star (*).

4 Click the Welcome tab.

The New Entry Queue IVR Service - Welcome dialog box opens.

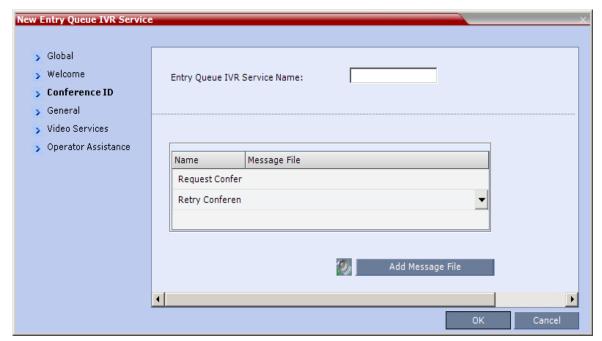




If the files were not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the Collaboration Server.

- 5 Define the appropriate parameters. This dialog box contains options that are identical to those in the Conference IVR Service - Welcome Message dialog box. For more information about these parameters, see New Conference IVR Service Properties - Conference Chairperson Options and Messages.
- 6 Click the Conference ID tab.

The New Entry Queue IVR Service - Conference ID dialog box opens.



7 Select the voice messages:

Entry Queue IVR Service Properties - Conference ID

Field/Option	Description
Request Conference ID	Prompts the participant for the conference ID.
Retry Conference ID	When the participant entered an incorrect conference ID, requests the participant to enter the ID again.

- **8** Assign an audio file to each message type, as follows:
 - ➤ In the **Message File** column, click the table entry, and then select the appropriate audio message.
- 9 Click the General tab.



The New Entry Queue IVR Service - General dialog box opens.

The administrator can enable an audio message that informs the participant of the lack of **Video Resources** in the *Collaboration Server* and that he/she is being connected as **Audio Only**. The message states: **All video resources are currently in use. Connecting using audio only**.

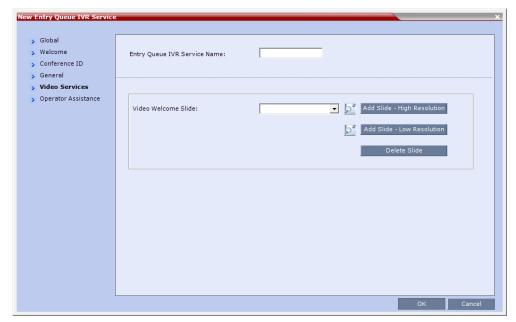
The following guidelines apply:

- > The **IVR** message applies to video participants only. **Audio Only** participants will not receive the message.
- > Only **H.323** and **SIP** participants receive the audio message.
- Downgrade to Audio Only is not supported for undefined ISDN dial in participants. These participants are disconnected if there is a lack of Video Resources (not supported with Collaboration Server 1800).
- The audio message is the first message after the call is connected, preceding all other IVR messages.
- ➤ The message is called **No Video Resources-Audio Only** and the message file (.wav) is called **No video resources audio only.wav**.
- The audio message must be added to the Conference and Entry Queue IVR Services separately.
- The IVR message can be enabled/disabled by the administrator using the ENABLE_ NO_VIDEO_RESOURCES_ AUDIO_ONLY_MESSAGE System Flag in system.cfg.

Possible values: YES / NO, default: YES

If you wish to modify the flag value, the flag must be added to the **System Configuration** file. For more information see the Modifying System Flags.

- 10 Enter the message Name and Message File name for the Audio Only message:
 - Message Name: No Video Resources-Audio Only
 - Message File name: No_Video_Resources_Audio_Only.wav
- 11 Click the Video Services tab.



The New Entry Queue IVR Service - Video Services dialog box opens.

- 12 In the Video Welcome Slide list, select the video slide that will be displayed to participants connecting to the Entry Queue. The slide list includes the video slides that were previously uploaded to the MCU memory.
- 13 To view any slide, click **Preview Slide** ().
- 14 If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click the:
 - Add Slide Low Resolution button to upload a Low Resolution Slide.
 - > Add Slide High Resolution button to upload a High Resolution Slide.

The **Install File** dialog box opens. The uploading process is similar to the uploading of audio files. For more information, see step 6.



The video slide must be in a .jpg or .bmp file format. For more information, see Creating a Welcome Video Slide.

15 Click the Operator Assistance tab.

The **Operator Assistance** dialog box opens.



- **16** Select **Enable Operator Assistance** to enable operator assistance when the participant requires or requests help during the connection process.
- **17** In the **Operator Assistance Indication Message** field, select the audio message to be played when the participant requests or is waiting for operator's assistance.



If the audio file was not uploaded prior to the definition of the IVR Service or if you want to add new audio files, click **Add Message File** to upload the appropriate audio file to the Collaboration Server.

- **18** Click **OK** to complete the Entry Queue Service definition.
- 19 The new Entry Queue IVR Service is added to the IVR Services list. For more information, see IVR Services List.

Setting a Conference IVR Service or Entry Queue IVR Service as the Default Service

The first Conference IVR Service and Entry Queue IVR Service are automatically selected by default. The IVR Services (Conference and Entry Queue) shipped with the system are also set as default. If additional Conference IVR Services and Entry Queue IVR Services are defined, you can set another service as the default for each service type.

To select the default Conference IVR Service:

• In the IVR Services list, select the Conference IVR Service to be defined as the default, and then click Set Default Conference IVR Service ().

IVR Services (3) Conferences (3) 🤹 💥 💽 🖃 唧齿×齿◆耳刀 Display Name Status ID Start Tim E Name Language Service Type 😩 SUPPORT 99466 1:02 PM Conference IVR Service Enalish Conference IVR Service Delete Service 😪 Marketing 46630 3:52 PM # 6 : iet Default Conference IVR Service 🌺 Logistics 43974 3:51 PM : 🟥 Entry Queue IVR Ser ervice Add Supported Languages Replace/Change Music File Properties RMX Management \triangle A Users Signaling Monitor 🥡 Hardware Monitor Meeting Rooms Participant Alerts Port Usage: Voice 1 / 50 Video 35 / 70 1

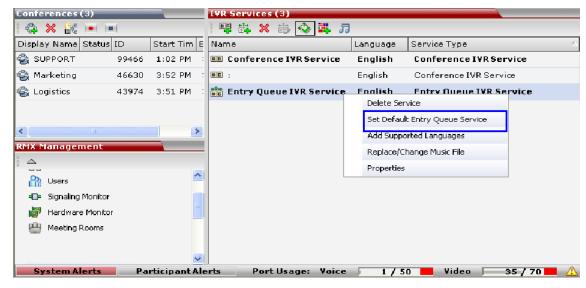
Alternatively, in the **IVR Services** list, right-click the Conference IVR Service and then select **Set Default Conference IVR Service**.

The IVR Service is displayed in bold, indicating that it is the current default service.

To select the Default Entry Queue IVR Service:

In the IVR Services list, select the Entry Queue IVR Service to be defined as the default, and then click Set Default Entry Queue IVR Service ().

Alternatively, in the **Conference IVR Services** list, right-click the Entry Queue IVR Service and then select **Set Default Entry Queue IVR Service**.



The default Entry Queue IVR Service is displayed in bold, indicating that it is the current default service.

Modifying the Conference or Entry Queue IVR Service Properties

You can modify the properties of an existing IVR Service, except the service name and language.

To modify the properties of an IVR Service:

- 1 In the RMX Management pane, click IVR Services.
- 2 In the IVR Services list, Click the IVR Service to modify.
 For more information about the tabs and options of this dialog box, see Defining a New Conference IVR Service.
- 3 Modify the required parameters or upload the required audio files.
- 4 Click OK.

Replacing the Music File

The Collaboration Server is shipped with a default music file that is played when participants are placed on hold, for example, while waiting for the chairperson to connect to the conference (if the conference requires a chairperson), or when a single participant is connected to the conference. You can replace the default music file with your own recorded music.

Music file guidelines:

- The file must be in *.wav format.
- Music length cannot exceed one hour.
- The music recording must be in the range of (-12dB) to (-9dB).

Adding a Music File

To replace the Music file:

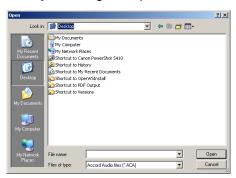
- 1 In the RMX Management pane, click IVR Services.
- 2 In the IVR Services list toolbar, click the Replace/Change Music File (3) button.

The Install Music File window opens.



3 Click the **Browse** button to select the audio file (*.wav) to upload.

The **Open** dialog box opens.



- 4 Select the appropriate audio *.wav file and then click Open.
 - The selected file name is displayed in the **Install Music File** dialog box.
- 5 You can play the selected file by clicking **Play** (**9**).
 - a Click Play Selected File to play a file on your computer.
 - **b** Click **Play RMX File** to play a file already uploaded on the **RMX**.
- 6 In the Install Music File dialog box, click OK to upload the file to the MCU.
- 7 The new file replaces the previously uploaded file and this file is used for all background music played by the MCU.

Creating Audio Prompts and Video Slides

The Collaboration Server is shipped with default voice messages (in WAV format) and video slides that are used for the default IVR services. You can create your own video slides and record the voice messages for different languages or customize them to your needs.

Recording an Audio Message

To record audio messages, use any sound recording utility available in your computer or record them professionally in a recording studio. Make sure that recorded message can be saved as a Wave file (*.wav format) and that the recorded format settings are as defined in steps 4 and 5 on the following procedure. The files are converted into the *Collaboration Server* internal format during the upload process.

This section describes the use of the Sound Recorder utility delivered with Windows 95/98/2000/XP.

To define the format settings for audio messages:



- The format settings for audio messages need to be set only once. The settings will then be applied to any new audio messages recorded.
- The utility or facility used to record audio messages must be capable of producing audio files with the formats and attributes as shown in the following procedure, namely, PCM, 16.000kHz, 16Bit, Mono.

Windows® XP® Sound Recorder is one of the utilities that can be used.

1 On your PC, select Start > Programs > Accessories > Entertainment > Sound Recorder.

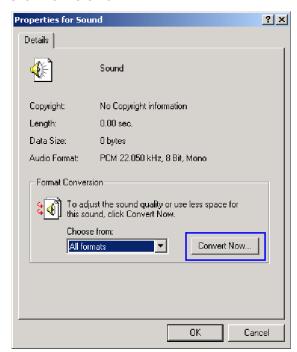
The Sound-Sound Recorder dialog box opens.



2 To define the recording format, click File > Properties.

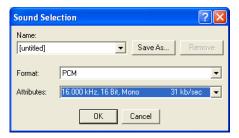
The **Properties for Sound** dialog box opens.

3 Click Convert Now.



The **Sound Selection** dialog box opens.

- 4 In the Format field, select PCM.
- 5 In the Attributes list, select 16.000 kHz, 16Bit, Mono.



6 To save this format, click the **Save As** button.

The **Save As** dialog box opens.

7 Select the location where the format will reside, enter a name and then click OK.



The system returns to the **Sound Selection** dialog box.

8 Click OK.

The system returns to the **Properties for Sound** dialog box.

9 Click OK.

The system returns to the Sound–Sound Recorder dialog box. You are now ready to record your voice message.

To record a new audio message:



Regardless of the recording utility you are using, verify that any new audio message recorded adheres to the following format settings: 16.000kHz, 16Bit, Mono.

Make sure that a microphone or a sound input device is connected to your PC.

- 1 On your PC, click Start > Programs > Accessories > Entertainment > Sound Recorder. The Sound-Sound Recorder dialog box opens.
- 2 Click File > New.
- 3 Click the Record button.

The system starts recording.

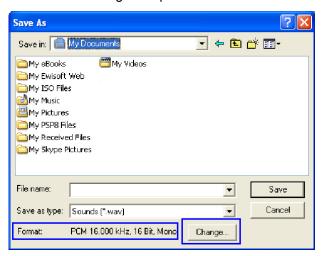
4 Start narrating the desired message.



For all audio IVR messages, stop the recording anytime up to 3 minutes (which is the maximum duration allowed for an IVR voice message). If the message exceeds 3 minutes it will be rejected by the Collaboration Server unit.

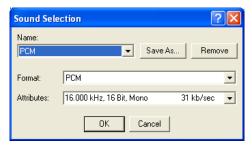
- 5 Click the Stop Recording button.
- 6 Save the recorded message as a wave file, click File > Save As.

The Save As dialog box opens.



7 Verify that the Format reads: PCM 16.000 kHz, 16Bit, Mono. If the format is correct, continue with step 10. If the format is incorrect, click Change.

The **Sound Selection** dialog box is displayed.



- 8 In the Name field, select the name of the format created in step step 7.
- 9 Click OK.

The system returns to the Save As dialog box.

- 10 In the Save in field, select the directory where the file will be stored.
- 11 In the Save as Type field, select the *.wav file format.
- 12 In the File name box, type a name for the message file, and then click the Save button.
- **13** To record additional messages, repeat steps 1 to 10.



To upload your recorded *.wav file to the Collaboration Server, see step 6.

Creating a Welcome Video Slide

The video slide is a still picture that can be created in any graphic application.

To create a welcome video slide:

- 1 Using any graphic application, save your image in either *.jpg or *.bmp file format.
- 2 For optimum quality, ensure that the image dimensions adhere to the Collaboration Server recommended values (width x height in pixels):
 - > 640 x 480
 - > 704 x 480
 - > 848 x 480
 - > 720 x 576
 - > 704 x 576
 - > 1024 x 576
 - > 960 x 720
 - > 1280 x 720
 - > 1440 x 1088
 - > 1920 x 1088

The Collaboration Server can accommodate small deviations from the recommended slide resolutions.

3 Save your file.



Customized H.261 slides are not supported..



If using a default Polycom slide, the slide's resolution will be as defined in the profile, i.e. SD, HD or CIF

If the display of the Welcome slide is cut in the upper area of the screen, change the settings of the endpoint's monitor to People **Stretch** instead of **Zoom**.



To upload your video slide to the Collaboration Server, see step 12.

Inviting Participants using DTMF



This feature is disabled in SVC conferences and for SVC participants in mixed CP and SVC conferences.

A participant in a video or audio conference can invite another participant to the conference using the touch-tone DTMF numeric keypad on the participant's endpoint. You can invite a participant using various communication devices, such as a mobile phone, an IP phone, PSTN phones, laptops, or connect to another conference running on another PBX or MCU.

Invite Call Flow

The following flow describes how a participant is invited to the conference using the DTMF codes:

- 1 During the conference, the participant enters the DTMF code (default is *72) on the numeric keypad to invite another participant.
- 2 The participant is prompted to enter the invited participant's destination number (a number or IP address) including the prefix (if required) and the DTMF delimiter digit ('*' or '#') at the end. The asterisk ('*') is used to denote the dot in the IP address.

For example: To enter an IP address such as 10.245.22.19, on the DTMF keypad press 10*245*22*19 and then the DTMF delimiter.



Digits that are entered after the DTMF delimiter and before the participant is connected are ignored.

- 3 The system automatically dials to the destination according to the protocol order as defined in the IVR Services Properties Video Services tab.
 - When the call cannot be completed by the current protocol, the system attempts to connect to the destination using the next protocol according to the protocol order.
 - The Collaboration Server connects the participant when the call is answered.
- 4 The last invited participant can be disconnected when the inviting participant enters the DTMF code (default is **#72**) on the numeric keypad.

Entering Additional DTMF Codes

In some environments, the call is answered by an IVR system (for example when connecting to another conference or PBX), requesting a password or a destination number to complete the connection process. In such a case, additional DTMF digits must be entered before the **DTMF forward duration** time has expired and are forwarded to the invited destination. When the additional DTMF codes are entered, they are heard by all the conference participants.

If the DTMF code is not entered on time or if the wrong DTMF code is entered, the participant is prompted for a new input. After the defined number of retries have elapsed, the call is ended.

Error Handling

• If the destination endpoint is busy or the participant did not answer, the system ends the call.

- When an incorrect number is entered, the call fails and an error message is displayed.
- If the destination number is not entered in a specific amount of time (defined in Timeout for user input in the IVR Services Global tab), the participant is prompted to enter a destination number again. Depending on the Number of user input retries as defined in the IVR Services Global tab, the system will attempt to receive the required input. When all the retries have failed, the call to the invited participant is cancelled.

Guidelines

- Inviting other participants is available to AVC-enabled participants only.
- Participants can be invited to Event Mode, and CP and VSW conferences.
- All network protocols are supported (H.323, SIP, ISDN, and PSTN). It is recommended to select PSTN and not ISDN if PSTN is the only destination protocol. If both PSTN and ISDN are enabled, it is recommended to select the PSTN before ISDN as the connection process for PSTN endpoints will be quicker.
- In an Multiple IP Networks environment, the system will try to connect the participant using each of
 the IP Network Services listed in the Conference Profile Network Services dialog box. Network
 services that are excluded from this list are skipped during the dialing sequence.
- In Event Mode conferences, the invited participant connection parameters must match one of the conference levels.
- In CP conferences, the participant initiating the invitation to another participant is able to view the dialing information and connection status. During the dialing process, the dialing string is displayed as the participant name which is replaced by the site name when connected to the conference.
- By default, all participants (Everyone) are granted permission to invite a participant to join a conference. To change the permission to the Chairperson, modify the **Permission** column in the **IVR Service - DTMF Codes** tab.

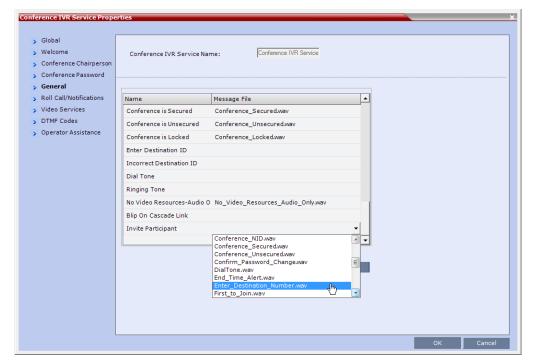
Enabling the Invite Participants using DTMF Option

The option to invite participants to a conference using the DTMF keypad is enabled in the following **Conference IVR Services** dialog boxes:

- General
- Video Services
- DTMF Codes

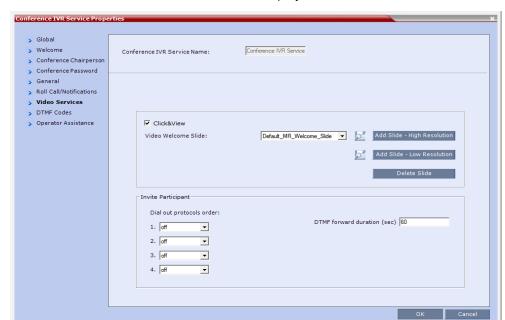
To enable the Invite Participant using DTMF on the Collaboration Server:

- 1 Open an existing or define a new Conference IVR Service.
 - Conference IVR Service Global dialog box opens.
- Click the General tab.



The Conference IVR Services - General tab is displayed.

- 3 In the Message File column of the Invite Participant entry, click the drop-down arrow and select the required voice message. The file Enter_Destination_Number.wav that is shipped with the system can be used for this message.
 - To upload a new file, click the **Add Message File**. For more details, see the Creating Audio Prompts and Video Slides.
- 4 Click the Video Services tab.



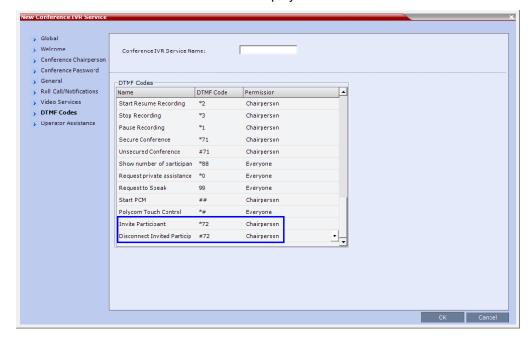
The IVR Services - Video Services tab is displayed.

5 Define the following parameters:

IVR Services Properties - Video Services Parameters - Invite Participants

Video Services	Description
Dial out protocols order	Select the order of the network protocols that will be used by the system to dial the destination number. The system will start dialing using the first protocol, and if the call is not answered it will continue with the second, third and fourth protocols (if they are enabled) until the call is answered. By default, H.323 is set as the first protocol and SIP as the second while the remaining protocols are disabled (set to Off). For PSTN calls, select the PSTN protocol and not ISDN. Set PSTN before ISDN if both PSTN and ISDN protocols are required.
DTMF forward duration	Use this field when connecting to another conferencing entity with an IVR, requiring the input of a password, destination number or ID. Enter the number of seconds that the system will wait for the input of additional DTMF digits such as a password or conference number. The range can be from 10 seconds to 600 seconds. Default is 60 seconds.

6 Click the DTMF Codes tab.



The IVR Services - DTMF Codes tab is displayed.

- 7 Make sure that Invite Participant and Disconnect Invited Participant have DTMF Codes assigned to them. Default system values are *72 (Invite Participant) and #72 (Disconnect Invited Participant), however you can enter your own values.
 - When upgrading from a previous version, default system values may not be assigned if these IVR entries were not defined in your existing IVR Service and have to be manually added to the **DTMF Codes** table.
- **8** If required, determine who can invite other participants to the conference using DTMF codes by changing the permissions to either **Chairperson** or **Everyone**.
- 9 Click OK.

Disabling the Invite Participant Option

To disable the Invite Participant option:

- 1 From the IVR Services DTMF Codes tab, delete the DTMF digits from the DTMF Code column.
- 2 Click OK.

External IVR Service Control

IVR Services can be controlled externally from an application server supporting the MCCF-IVR (Media Control Channel Framework-Interactive Voice Response) package. The external IVR service is currently being implemented with the integration of the Polycom RealPresence Virtualization Manager (DMA) as the application server. When the application server is deployed in the enterprise environment and the Polycom RealPresence Collaboration Server (MCU) is deployed as a media server, the external IVR service can be used to play audio messages, display slides, and collect DTMF input from the participant.

For more information, see Using External IVR Services via the MCCF-IVR Package.

IVR Services Support with TIP Protocol

From Version 8.1, Conference IVR and Entry Queue IVR Services are supported with AVC TIP protocol in conferences that include both TIP-enabled and non-TIP-enabled endpoints. TIP-enabled endpoints can be moved from the Entry Queue to the destination conference if the **TIP Compatibility Modes** settings in the Profile are identical for both conferencing entities (it is recommended to use the same **Profile** for both entities).

The IVR services can be enabled for all TIP Compatibility Modes:

- Video only
- Video and Content
- Prefer TIP

IVR media files, WAV for voice messages and JPG for video slides, are all stored on the RealPresence Collaboration Server (RMX).

Guidelines for TIP Support with IVR Services

- AVC SIP and TIP protocols are supported on the RealPresence Collaboration Server 1500/2000/4000 only.
- IVR default audio files are enabled for all **TIP Compatibility Modes**.
- Only Polycom default Welcome slides are available. Custom Welcome slides are not supported.
- TIP-enabled endpoints can send DTMF digits to MCU.
- In an mixed TIP environment, there is no support for content in cascaded conferences. Additionally, Legacy and Lync endpoints cannot view content.

Default IVR Prompts and Messages

The system is shipped with the following audio prompts and messages:

Default IVR Messages

Message Type	Message Text	When Played	File Name
General Welcome Message	Welcome to unified conferencing.	The participant enters the conference IVR queue	General_Welcome.wav
Chairperson Identifier Request	For conference Chairperson Services, Press the Pound Key. All other participants please wait	The participant is asked to self-identify as the chairperson	Chairperson_ Identifier.wav
Request Chairperson Password	Please enter the Conference Chairperson Password. Press the pound key when complete.	The participant is asked for the chairperson password	Chairperson_Password.wav
Retry Chairperson Password	Invalid chairperson password. Please try again.	A participant enters an incorrect Chairperson password	Chairperson_Password_Failure. wav
Request Password	Please enter the conference password. Press the pound key when complete.	A participant is requested to enter the conference password	Conference_ Password.wav
Retry Password	Invalid conference password. Please try again.	An incorrect conference password is entered	Retry_ Conference_Password.wav
Request Digit	Press any key to enter the conference.	A participant is requested to press any key	Request_Digit.wav
Request Billing Code	Please enter the Billing code. Press the pound key when complete.	A participant is asked to enter a billing code	Billing_Code.wav
Requires Chairperson	Please wait for the chairperson to join the conference.	A participant attempts to join a conference prior to the Chairperson joining	Requires Chairperson.wav

Default IVR Messages

Message Type	Message Text	When Played	File Name
Chairperson Exit	The chairperson has left the conference. Note: The TERMINATE_CONF_AFTER_CHAIR _DROPPED flag must be enabled to play this message.	The chairperson has left the conference.	Chairperson_Exit.wav
First to Join	You are the first person to join the conference.	The first participant joins a conference	First to Join.wav
Mute All On	All conference participants are now muted.	When all participants are muted by the operator or chairperson.	Mute_All_On.wav
Mute All Off	All conference participants are now unmuted.	When all participants are unmuted by the operator or chairperson.	Mute_All_Off.wav
End Time Alert	The conference is about to end.	The conference is about it end	End_Time_Alert.wav
Change Password Menu	Press one to change conference password. Press two to change chairperson password. Press nine to exit the menu.	A participant requests a conference password change	Change_Password_ Menu.wav
Change Conference Password	Please enter the new conference password. Press the pound key when complete.	A participant presses two in the Change Password IVR menu.	Change_ Conference_Password.wav
Change Chairperson Password	Please enter the new chairperson password. Press the pound key when complete.	A participant presses one in the Change Password IVR menu.	Change_ Chairperson_Password.wav
Confirm Password Change	Please re-enter the new password. Press the pound key when complete.	A participant enters a new conference or chairperson password	Confirm_ Password_Change.wav

Default IVR Messages

Message Type	Message Text	When Played	File Name
Change Password Failure	The new password is invalid.	A participant enters an invalid password	Change_ Password_Failure.wav
Password Changed Successfully	The password has been successfully changed.	A participant has confirmed a password change	Password_ Changed_Successfully.wav
Self Mute	You are now muted.	A participant mutes his or her audio	Self_Mute.wav
Self Unmute	You are no longer muted.	A participant unmutes his or her audio	Self_Unmute.wav
Chairperson	 The available touch-tone keypad actions are as follows: To exit this menu press any key. To request private assistance, press star, zero. To request operator's assistance for the conference, press zero, zero. To mute your line, press star, six. To unmute your line, press pound, 	A chairperson requests the chairperson help menu	Chairperson_ Help_Menu.wav
Participant Help Menu	six. The available touch-tone keypad actions are as follows: To exit this menu press any key. To request private assistance, press star, zero. To mute your line, press star, six. To unmute your line, press pound, six. To increase your volume, press star, nine. To decrease your volume, press pound, nine.	A participant requests the participant help menu	Participant_Help_Menu.wav
Maximum Participants Exceeded	The conference is full. You cannot join at this time.	A participant attempts to join a full conference	Maximum_ Participants_Exceeded.wav
Roll Call Record	After the tone, please state your name.		Roll_Call_Record.wav
Roll Call Joined	has joined the conference.		Roll_Call _Joined.wav
Roll Call Left	has left the conference.		Roll_Call_Left.wav

Default IVR Messages

Message Type	Message Text	When Played	File Name
Roll Call Review	The conference participants are		Roll_Call_ Review.wav
Request Conference NID	"Please enter your conference NID. Press the pound key when complete.		Request_ Conference_NID.wav
Retry Conference NID	Invalid conference NID. Please try again.	A participant enters an invalid conference NID	Retry_Conference_NID.wav
Secured Conference	The conference is now secured.	A chairperson or participant secures a conference	Conference_Secured.wav
Unsecured Conference	The conference is now in an unsecured mode	A chairperson or participant unsecures a conference	Conference_Unsecured.wav
Locked Conference	Conference you are trying to join is locked		Conference_Locked.wav
Conference Recording	The conference is being recorded		Recording_ in_Progress.wav
Conference Recording Failed	The conference recording has failed		Recording_Failed.wav
No Video Resources Audio Only.	All video resources are currently in use. Connecting using audio only		No_Video_Resources_Audio_O nly.wav

Volume Control of IVR Messages, Roll Call and Music

The volume of IVR music, and IVR messages and Roll Call is controlled by the following system flags:

- IVR_MUSIC_VOLUME
- IVR_MESSAGE_VOLUME
- IVR_ROLL_CALL_VOLUME

To control the volume of IVR music, Roll Call and messages:

 Modify the values of the System Flags listed in the following table by selecting Setup > System Configuration.

If these flags do not appear in the *System Flags* list, they must be manually added. For more information see *System Configuration Flags*.

Default IVR Messages

Flag	Description
IVR_MUSIC_VOLUME	The volume of the IVR music played when a single participant is connected to the conference varies according to the value of this flag. Possible value range: 0-10 (Default: 2). 0 – disables playing the music 1 – lowest volume 10 – highest volume
IVR_MESSAGE_VOLUME	The volume of IVR messages varies according to the value of this flag. Possible value range: 0-10 (Default: 2). 0 – disables playing the IVR messages 1 – lowest volume 10 – highest volume Note: It is not recommended to disable IVR messages by setting the flag value to 0.
IVR_ROLL_CALL_VOLUME	The volume of the Roll Call varies according to the value of this flag. Possible value range: 0-10 (Default: 4). 0 – disables playing the Roll Call 1 – lowest volume 10 – highest volume Note: It is not recommended to disable the Roll Call by setting the flag value to 0.



The following System Flags do not require an MCU reset:

- IVR_MESSAGE_VOLUME
- IVR_MUSIC_VOLUME
- IVR_ROLL_CALL_VOLUME

For all other flag changes, the MCU must be reset for the modified flag settings (including deletion) to take effect.

IVR Services in TIP-Enabled Conferences

Conference IVR and Entry Queue/Virtual Entry Queues are supported with AVC TIP protocol in conferences that include both TIP-enabled and non-TIP-enabled endpoints.

A Virtual Entry Queue can be configured to either IVR Only Service Provider or External IVR Control mode.

TIP-enabled endpoints can be moved from the Entry Queue to the destination conference if the **TIP Compatibility Modes** settings in the Profile are identical for both conferencing entities (it is recommended to use the same **Profile** for both entities).

TIP IVR users can access the conference directly or enter the Entry Queue/Virtual Entry Queue and provide a password to access the conference.

The IVR services can be enabled for all TIP Compatibility Modes:

- Video only
- Video and Content
- Prefer TIP

IVR media files, WAV for voice messages and JPG for video slides, are all stored on the RealPresence Collaboration Server (RMX).

IVR Services in TIP-Enabled Conferences Guidelines

- IVR default audio files are enabled for all TIP Compatibility Modes.
- Only Polycom default Welcome slides are available. Custom Welcome slides are not supported.
- TIP-enabled endpoints can send DTMF digits to MCU.
- In a mixed TIP environment there is no support for content in cascaded conferences. Additionally, Legacy and Lync endpoints cannot view content.

Entry Queue and Virtual Entry Queue Access

TIP endpoints can dial-in to conferences directly using the IVR, Entry Queue/Virtual Entry Queue and IVR Only Service Provider. For more information see Defining a New Entry Queue

For more information on Multipoint see the Collaboration With Cisco's Telepresence Interoperability Protocol (TIP).

Configuring the Conference and Entry Queue IVR Services

The IVR module includes two types of services:

- Conference IVR Service that is used with conferences
- Entry Queue IVR Service that is used with Entry Queues

The configuration process is the same for TIP and non-TIP enabled Conferences and Entry Queues.

For more information about IVR Services see, Defining a New Conference IVR Service.

For more information about Entry Queues see, Entry Queues.

For more information see Appendix I - Polycom Open Collaboration Network (POCN).

Call Detail Record (CDR) Utility

The Call Detail Record (CDR) utility enables you to view summary information about conferences, and retrieve full conference information and archive it to a file. The file can be used to produce reports or can be exported to external billing programs.



The value of the fields that support Unicode values, such as the info fields, will be stored in the CDR file in UTF8. The application that reads the CDR must support Unicode.

The Collaboration Server can store details of up to 2000 (RealPresence Collaboration Server (RMX) 1500/1800/2000) or 4000 (RealPresence Collaboration Server (RMX) 4000)conferences. When this number is exceeded, the system overwrites conferences, starting with the earliest conference. To save the conferences' information, their data must be retrieved and archived. The frequency with which the archiving should be performed depends on the volume of conferences run by the MCU.

The Collaboration Server displays Active Alarms before overwriting the older files, enabling the users to backup the older files before they are deleted. The display of Active Alarms is controlled by the **ENABLE_CYCLIC_FILE_SYSTEM_ALARMS** system flag.

If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE system flag is set to YES) and a Cyclic File reaches a file storage capacity limit, an Active Alarm is created: Backup of CDR files is required.

Each conference is a separate record in the MCU memory. Each conference is archived as a separate file. Each conference CDR file contains general information about the conference, such as the conference name, ID, start time and duration, as well as information about events occurring during the conference, such as adding a new participant, disconnecting a participant or extending the length of the conference.

The CDR File Properties

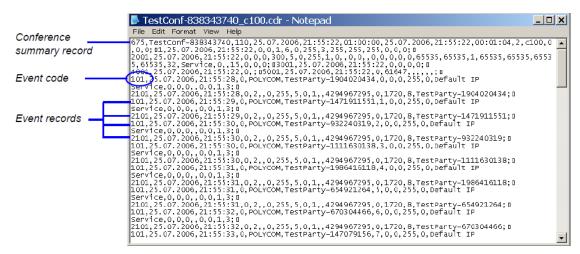
The output of a CDR file depends on the format in which the file was archived and the size of the file.

CDR File Formats

The conference CDR records can be retrieved and archived in the following two formats:

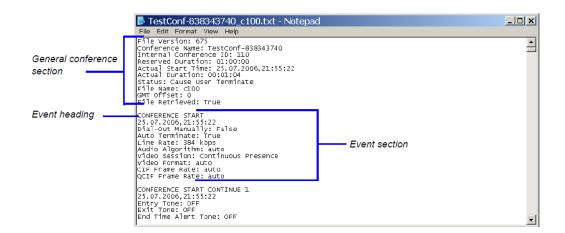
Unformatted data – Unformatted CDR files contain multiple records in raw data format. The first
record in each file contains general conference data. The remaining records contain event data, one
record for each event. Each record contains field values separated by commas. This data can be
transferred to an external program such as Microsoft Excel® for billing purposes. The following is a
sample of an unformatted CDR file.

Unformatted CDR File



Formatted text – Formatted CDR files contain multiple sections. The first section in each file contains
general conference data. The remaining sections contain event data, one section for each event.
Each field value is displayed in a separate line, together with its name. This data can be used to
generate a summary report for a conference. The following is an example of a formatted CDR file.

Formatted CDR File





The field names and values in the formatted file will appear in the language being used for the Collaboration Server Web Client user interface at the time when the CDR information is retrieved.

Multi-Part CDR Files

By default, the maximum CDR (Call Data Record) file size is limited to 1MB. When a CDR file reaches a size of 1MB the file is saved and further call data recording is stopped and the additional data is lost.

The Collaboration Server can be configured to keep recording the data in multiple CDR file set of 1MB each. Multi-Part CDR ensures that conference call data from long duration or permanent conferences is recorded and not lost.

Enabling the Multi-Part CDR Option

 Multi-Part CDR is enabled by setting the value of the ENABLE_MULTI_PART_CDR system flag to YES.

The flag's default value is NO.

When the flag value is **NO**, CDR file size is limited to one file of 1MB and further call data recording is stopped.

To modify the default setting, the flag must be manually added to the System Configuration. For more information see, Modifying System Flags.

- If the flag value is set to YES, when a CDR file reaches 1MB, an additional CDR file is created and added to the CDR file set for that conference.
- If the flag value is changed from YES to NO (or visa versa) all existing CDR files are retained.

CDR File Contents

The general conference section or record contains information such as the Routing Name and ID, and the conference starting date and time.

The event sections or records contain an event type heading or event type code, followed by event data. For example, an event type may be that a participant connects to the conference, and the event data will list the date and time the participant connects to the conference, the participant name and ID, and the participant capabilities used to connect to the conference.

To enable compatibility for applications that written for the MGC family, the *Collaboration Server* CDR file structure is based on the MGC CDR file structure.

The unformatted and formatted text files contain basically the same information. The following differences should be noted between the contents of the unformatted and formatted text files:

- In many cases a formatted text file field contains a textual value, whereas the equivalent unformatted file field contains a numeric value that represents the textual value.
- For reading clarity, in a few instances, a single field in the unformatted file is converted to multiple
 fields in the formatted text file, and in other cases, multiple fields in the unformatted file are combined
 into one field in the formatted file.
- To enable compatibility between MGC CDR files and Collaboration Server CDR files, the unformatted
 file contains fields that were applicable to the MGC MCUs, but are not supported by the Collaboration
 Server MCUs. These fields are omitted from the formatted text file.



Appendix C - CDR Fields, Unformatted File Appendix contains a full list of the events, fields and values that appear in the unformatted file. This appendix can be referred to for information regarding the contents of fields in the unformatted text file, but does not reflect the exact contents of the formatted text file.

Viewing, Retrieving and Archiving Conference Information

You can view the list of CDR files and retrieve them to your local workstation. These files can then be used to generate billing information, resource usage reports and more by any third party application.

Viewing the Conference Records

You can list all the CDR files that are currently saved on the MCU.

To open the CDR utility:

» On the Collaboration Server Menu, click **Administration > CDR**.

The **CDR List** pane opens, displaying a list of the conference CDR records stored in the MCU memory.



The following fields are displayed:

Conference Record Fields

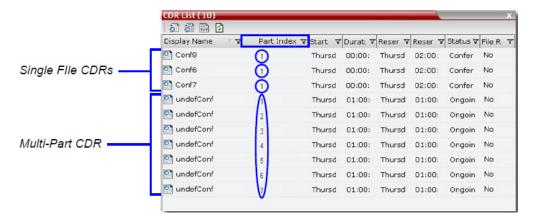
Field	Description	
Display Name	The Display Name of the conference and an icon indicating whether or not the CDR record has been retrieved and saved to a formatted text file. The following icons are used:	
	The CDR record has not been saved.	
	The CDR record has been saved.	
Start Time	The actual time the conference started.	

Conference Record Fields (Continued)

Field	Description	
GMT Start Time	The actual time the conference started according to Greenwich Mean Time (GMT).	
Duration	The actual conference duration.	
Reserved Start Time	The reserved start time of the conference. If the conference started immediately this is the same as the Start Time .	
Reserved Duration	The time the conference was scheduled to last. Discrepancy between the scheduled and the actual duration may indicate that the conference duration was prolonged or shortened.	
Status	 The conference status. The following values may be displayed: Ongoing Conference Terminated by User Terminated when end time passed Automatically terminated when conference was empty – The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. Conference never became ongoing due to a problem Unknown error Note: If the conference was terminated by an MCU reset, the status Ongoing Conference will be displayed. 	
File Retrieved	Indicates if the conference record was downloaded using any of the file retrieval buttons in the CDR List pane or the API. • Yes - when the conference record was retrieved to any file or using the API. • No - when the conference record was not retrieved at all. The File Retrieved field is updated whenever the record is downloaded.	

Multi-part CDR File display

When the Multi-Part CDR is configured on the Collaboration Server, an additional column, **Part Index** is added to the CDR list.



The Part Index column displays the CDR file's sequence in the CDR file set:

- CDRs that are up to 1MB consist of a single file. Each file has a unique Display Name and a Part Index of 1.
- Files included in a Multi-Part CDR file sets have the same Display Name. The first file of the set is numbered 1 with each additional CDR file numbered in an ascending numeric sequence.

Refreshing the CDR List

If the CDR file list is displayed for sometime and you want the latest CDR files to be displayed, you can refresh the list.

To refresh the CDR list:

» Click the Refresh button, or right-click on any record and then select Refresh.
Updated conference CDR records are retrieved from the MCU memory.

Retrieving and Archiving Conference CDR Records

You can retrieve the CDR files and store them on your workstation for later use.

To retrieve and archive CDR records:

1 To retrieve a single CDR record, right-click the record to retrieve and then select the required format or select the record to retrieve, and then click the appropriate button on the toolbar as detailed in the following table.

To retrieve multiple CDR records simultaneously, use standard Windows multi-selection methods.

Menu Option	Button	Action
Retrieve	6	Retrieves the conference information as unformatted data into a file whose extension is .cdr.
Retrieve Formatted XML	<i>3</i>	Retrieves the conference information as formatted text into a file whose extension is .xml. Note: Viewed when logged in as a special support user.
Retrieve Formatted	TRT	Retrieves the conference information as formatted text into a file whose extension is .txt.

The **Retrieve** dialog box opens.

The dialog box displays the names of the destination CDR files.

2 Select the destination folder for the CDR files and then click **OK**.

If the destination file already exists, you will be asked if you want to overwrite the file or specify a new name for the destination file.

The files are saved to the selected folder.



CDR files are not included in the backup process and should be backed up manually by saving the CDR files to a destination device.

Gateway Calls



- Gateway calls are supported with AVC calls only.
- Gateway calls, ISDN Connections and Video Switching conferences are not supported with RealPresence Collaboration Server (RMX) 1800.

The RealPresence Collaboration Server (RMX) 1500/2000/4000 can be used as a gateway that provides connectivity across different physical networks and translates multiple protocols for point-to-point rich media communications.

The Collaboration Server supports the widest range of video and audio algorithms. It allows sites with different frame rates, connection speeds, audio algorithms, video resolutions and network protocols to transparently connect with one another. It also enables multipoint conference creation from an endpoint.

A special conference acting as a Gateway Session is created on the Collaboration Server. It includes one dial-in connection of the endpoint initiating the Gateway Session and one or several dial-out connections to endpoints. It provides connectivity between the various protocols: H.323, SIP, ISDN and PSTN.

To enable the gateway functionality a special Gateway Profile is defined on the Collaboration Server.

Gateway Functionality

The following features and capabilities are supported in gateway calls:

- Gateway Sessions are in CP Mode only.
 - If Video Switching is selected in the Profile assigned to the Gateway Session, the system ignores this setting and will run the Gateway Session in CP mode.
 - From Version 7.2, Gathering phase is not supported in gateway calls, even if it is defined in the Profile assigned to the Gateway Profile.
- Sharing Content using H.239 protocol
- FECC.

Note: Only IP participants can use FECC as it is not supported by the ISDN protocol.

Recording.

Note: The Recording Link is not considered as a participant and therefore, the gateway session will automatically end when only one of the participants remains connected in addition to the recording link. The video of the Recording Link is not included in the display of the video of the gateway call.

 Forwarding of DTMF codes from the Gateway Session to a conference running on another gateway, MCU or DMA. This enables the participant to enter the required conference and/or chairperson password when connecting to another conference.

DTMF forwarding is enabled when there are only two participants connected to the Gateway Session.

- Forwarding of all DTMF codes sent by participants in the Gateway Session to all PSTN and ISDN participants. This is enabled by adding the
 ALWAYS_FORWARD_DTMF_IN_GW_SESSION_TO_ISDN System Flag to system.cfg and setting its value to YES.
- Up to 80 gateway calls may be run on a fully configured MCU.
- Gateway Profiles are included in the Backup and Restore Configuration operations.
- CDR files are generated for Gateway Sessions in the same way as for conferences.
- Cascading. To support cascading, the gateway indicates a lower number than the MCU for master-slave relation (directly or through DMA).
- Gateway calls are supported in Microsoft and Avaya environments.
- If the ENABLE_AUTO_EXTENSION system flag is set to:
 - > YES (default), Gateway Calls are not limited in duration while endpoints are connected.
 - > NO, Gateway Calls are limited to 60 minutes.

For more information see Modifying System Flags.

Call Flows

Call flow changes according to the connection protocols: IP or ISDN. This section describes the call flows between two endpoints connect via one gateway. For call flows describing connections between two endpoints via two gateways, or a connection of an endpoint to a conference running on MCU via a gateway, see Basic Cascading using ISDN Cascaded Link.

IP Participants

The following calling methods are available:

- Direct Dialing the dialing string includes the destination number/conference ID and the call is routed directly to the destination endpoint/conference. This is the recommended method.
- Gateway IVR Dialing For IP Participants the call connects to the gateway, where through interaction with the IVR, the destination number is entered using DTMF codes.
- Direct Dialing Using IP Addresses dial and receive calls to and from H.323 endpoints using the IP address when that the Gatekeeper is not functioning
- Calling a SIP Endpoint in a Remote Domain connection of H.323 and SIP endpoints residing in one domain to SIP endpoints residing in a remote domain

Direct Dialing

The calling endpoint enters the dialing string that includes the access numbers to the Collaboration Server Gateway Profile and the number of the destination endpoint. Up to 10 destination numbers can be entered in one string.

The call connects to the Collaboration Server Gateway Profile and a Gateway Session is created. The dial-in participant is automatically connected to it.

During the connection phase, the number being dialed is displayed on the screen of the calling endpoint.

If the call is not answered or it cannot be completed using one communication protocol, the system will try to connect the endpoint using the next communication protocol according to the selected protocols in the following order: H.323, SIP and ISDN. PSTN numbers are identified separately and are dialed immediately without trying other connections.

If the call is busy, the system will not try to connect the endpoint using another protocol.

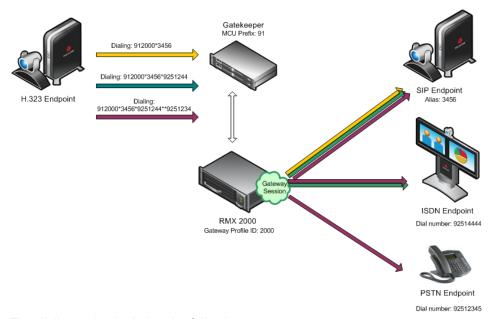
If the call is not completed after trying all possible protocols, the system displays the number that was dialed on the calling endpoint's screen and the reason for not completing the call. For details, see Connection Indications.

When the call is connected, a new Gateway Session is created and added to the ongoing Conferences list.

Dialing from H.323 Endpoints

The calling endpoints can dial to one, two or several endpoints (up to ten) in one dialing string.

Dialing String and Call Flow from H.323 Endpoint to One, Two or Three Endpoints



The dialing string includes the following components:

[MCU prefix in GK] - the prefix with which the Collaboration Server is registered to the gatekeeper. [GW Profile ID] - The ID of the Gateway Profile to be used for routing the call to the destination endpoint or DMA, as defined in the Collaboration Server Gateway Profiles. It includes the parameters of the call to the destination.

- *- indicates H.323, SIP or ISDN connection protocol to the destination endpoint (followed by the appropriate destination number). Placing this delimiter before the destination number causes the system to try to connect the endpoint using H.323 first, then SIP and lastly ISDN according to the selected protocols.
- ** indicates a PSTN connection to the destination endpoint (followed by the appropriate destination number).

[Destination number] - the destination number as alias, IPv4 address or ISDN/PSTN number.

The dialing string:

```
[MCU prefix in GK] [GW Profile ID]*[Destination Number, first participant]*[Destination Number, second participant]**[Destination number].....*[Destination Number, tenth participant]
```

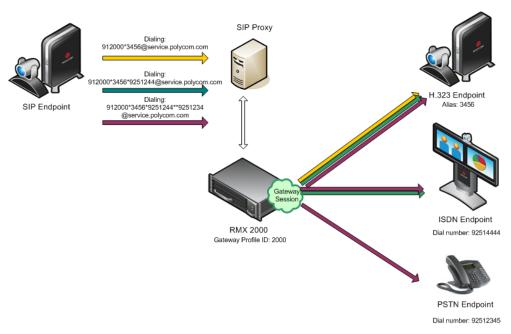
For example, If the MCU Prefix in the GK is 91 and the GW Profile ID is 2000, and the destination number is 3456 (SIP) enter: 912000*3456.

To invite two participants: SIP: 3456 and ISDN: 9251444, enter: 912000*3456*9251444.

To invite two participants: SIP: 3456 and a PSTN participant whose number is 9251234, enter: 912000*3456**9251234.

Dialing from SIP Endpoints

Dialing String and Call Flow from SIP Endpoint to One, Two or Three Endpoints



The calling endpoints can dial to one, two or several endpoints (up to ten) in one dialing string. The dialing string includes the following components:

[MCU Prefix in SIP Proxy] - The prefix with which the Collaboration Server is registered to the SIP Proxy. This component is optional and is not required in most cases.

[GW Profile ID] - The ID of the Gateway Profile to be used for routing the call to the destination endpoint or DMA, as defined in the Collaboration Server Gateway Profiles. It includes the parameters of the call to the destination.

- *- indicates H.323, SIP or ISDN connection protocol to the destination endpoint (followed by the appropriate destination number). Placing this delimiter before the destination number causes the system to try to connect the endpoint using H.323 first, then SIP and lastly ISDN according to the selected protocols.
- ** indicates a PSTN connection to the destination endpoint (followed by the appropriate destination number).

[Destination number] - the destination number as alias, IPv4 address or ISDN/PSTN number.

[@domain name] - the Collaboration Server domain name as registered to the SIP Proxy

The dialing string:

[GW Profile ID]*[Destination Number, first participant]*[Destination Number, second participant]**[destination number].....*[Destination Number, tenth participant]@domain name

Optional:

[GW Profile ID]*[Destination Number, first participant]*[Destination Number, second participant]**[destination number].....*[Destination Number, tenth participant]@IP address of the Collaboration Server signaling host

Optional:

[MCU prefix in SIP Proxy] [GW Profile ID]*[Destination Number, first participant]*[Destination Number, second participant]**[destination number].....*[Destination Number, tenth participant]@domain name

For example, if the GW Profile ID is 2000, the domain name is service.polycom.com, and the destination number is 3456, enter: 2000*3456@service.polycom.com.

If using the IP address of the Collaboration Server signaling host (for example, 172.22.188.22) instead of the domain name enter: 2000*3456@172.22.188.22.

To invite two participants IP: 3456 and ISDN: 9251444, enter: 2000*3456*9251444@service.polycom.com.

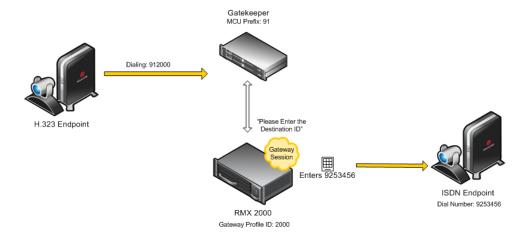
To invite two participants IP: 3456 and PSTN: 9251234, enter: 912000*3456**9251234@service.polycom.com.

Gateway IVR Dialing For IP Participants

Can be used by IP endpoints when the destination dialing string includes the address of the MCU only. This is the same flow as the dialing method used for ISDN/PSTN calls, however it is less recommended for IP participants. For details, see Dialing via Gateway IVR for ISDN Participants.

Dialing from H.323 Endpoints

Dialing String and Call Flow from IP Endpoint to ISDN Endpoint



[MCU prefix in GK] - the prefix with which the Collaboration Server is registered to the gatekeeper.

[GW Profile ID] - The ID of the Gateway Profile to be used for the gateway call and the IVR message.

The dialing string format is:

```
[MCU prefix in GK] [GW Profile ID]
```

For example, if the MCU Prefix in the GK is 91 and the GW Profile ID is 2000 enter: 912000.

Once the participant is connected to the Gateway Profile and hears the IVR message requesting the destination number, using the DTMF input keypad, the participant enters the number of the destination endpoint followed by the # key. PSTN numbers are identified by an * before the number.

For example, enter 3456# for IP endpoint, or 9253456# for ISDN, or *9253456# for PSTN phone.

To enter an IP address as the destination number, replace the periods (.) with asterisks (*) in the format n*n*n*n followed by the # key. For example, if the IP address is 172.22.188.22, enter 172*22*188*22#.

Dialing from SIP Endpoints

[MCU prefix in SIP Proxy] - the prefix with which the Collaboration Server is registered to the gatekeeper. [Optional.]

 $\begin{tabular}{ll} [GW \ Profile \ ID] \ - The \ ID \ of the \ Gateway \ Profile \ to be \ used for the \ gateway \ call \ and \ the \ IVR \ message. \end{tabular}$

[@domain name] - the Collaboration Server domain name as registered to the SIP Proxy.

The dialing string:

[GW Profile ID]@domain name

Optional:

[GW Profile ID]@IP address of the Collaboration Server signaling host

Optional:

```
[MCU prefix in SIP proxy] [GW Profile ID]@domain name
```

Once the participant is connected to the *Gateway Profile* and hears the IVR message requesting the destination number, using the DTMF input keypad, the participant enters the number of the destination endpoint followed by the # key. PSTN numbers are identified by an * before the number.

For example, enter 3456# for IP endpoint, or 9253456# for ISDN, or *9253456# for PSTN phone.

To enter an IP address as the destination number, replace the periods (.) with asterisks (*) in the format n*n*n*n followed by the # key. For example, if the IP address is 172.22.188.22, enter 172*22*188*22#.

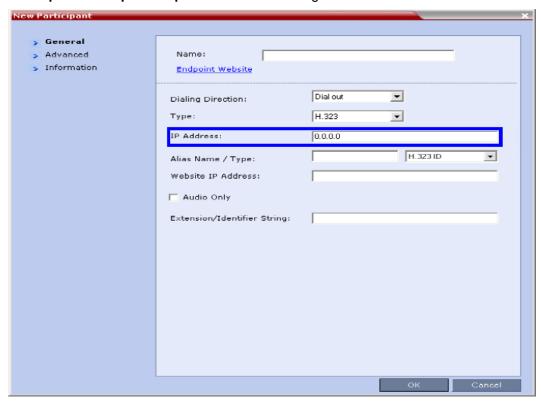
Direct Dialing Using IP Addresses

For Collaboration Servers registered to a gatekeeper, the Collaboration Server can be configured to dial and receive calls to and from H.323 endpoints using the IP address in the event that the Gatekeeper is not functioning.

Dial-out Calls

For Dial-out calls, direct IP dialing is enabled or disabled by the **GK_MANDATORY_FOR_CALLS_OUT** system flag.

When the flag is set to **NO** (default), if the Gatekeeper is not functioning, the Collaboration Server dials to the endpoint using the endpoint's IP address configured in the IP Address field of the **New Participant/Participant Properties - General** dialog box.



If no IP address is defined in the Participant Properties, the call will fail.

The method by which calls are dialed out to the endpoint is dependant on the flag value and the availability of the Gatekeeper as summarized in the following table:

Determination of Method for Dialing an Endpoint by Flag and Gatekeeper Availability

Flag Value	Gatekeeper Available	Results
NO	NO	Dial out to endpoint IP Address bypassing the Gatekeeper.
NO	YES	Dial out to endpoint Alias Name using the Gatekeeper.
YES	NO	No dial out to endpoint.
YES	YES	Dial out to endpoint Alias Name using the Gatekeeper.

Dial-in Calls

For Dial-in calls, direct IP dialing is enabled or disabled by the **GK_MANDATORY_FOR_CALLS_IN** and system flag.

When the flag is set to NO (default), if the Gatekeeper is not functioning, calls from endpoints will be connected directly to the Entry Queue, Conference or Meeting Room that was dialed.

The method by which dial-in calls are accepted or rejected is dependant on the flag value and the availability of the Gatekeeper as summarized in the following table.

GK_MANDATORY_FOR_CALLS_IN - System Flag

Flag Value	Gatekeeper Available	Results
NO	NO	Dial-in call is connected bypassing the Gatekeeper.
NO	YES	Dial-in call is connected using the Gatekeeper.
YES	NO	Dial-in call is rejected.
YES	YES	Dial-in call is connected using the Gatekeeper.

Enabling or Disabling Direct IP Dialing

The direct IP dialing is enabled by default. To disable it, manually add the flags

GK_MANDATORY_FOR_CALLS_OUT and GK_MANDATORY_FOR_CALLS_IN to the System

Configuration - MCMS_PARAMETERS dialog box and for each flag enter the required value (YES or NO).

For more information on flag definition, see Modifying System Flags.



For flag changes (including deletion) to take effect, reset the Collaboration Server. For more information see Resetting the Collaboration Server.

Calling a SIP Endpoint in a Remote Domain

The Gateway functionality allows the connection of H.323 and SIP endpoints residing in a domain, to SIP endpoints residing in a remote domain.

This functionality can be enabled when:

- The calling endpoint may be H.323 or SIP.
- The destination endpoint must be SIP.
- The dial string from the calling endpoint to the Collaboration Server includes the gateway dial-out number of the SIP endpoint that is located in the remote domain.

By definition, a dial-in string cannot contain two domains and it is therefore necessary that the dial string be of the following format:

mcu-meeting-room*dest%40dest-domain@mcu-domain

Where:

- The domain of the gateway call is mcu-domain
- The remote destination domain is dest%40dest-domain.
- The "%40" is replaced with an "@" when the gateway call is dialed to the remote SIP destination.



- · DTMF tones and Caller-id are not passed end-to-end.
- In order to support RTV, the SIP Server Type must be defined as Microsoft.

ISDN Participants

Two dialing methods are available to ISDN/PSTN participants:

- Dialing via Gateway IVR for ISDN Participants
- Direct Dial-in to Endpoints or DMA VMR using Automatically Generated Destination Numbers.
 This dialing method is available from Version 7.1.

In addition, PSTN participants can dial the Gateway IVR and can use the MCU or DMA prefix in the gatekeeper together with the conference ID/endpoint alias as the destination string to simplify the input. This is one of the methods for PSTN participants to connect to a virtual Meeting Room on the DMA.

Dialing via Gateway IVR for ISDN Participants

In this flow, the calling endpoint enters the dialing string that includes the access number to the Collaboration Server Gateway Profile.

The endpoint connects to the Collaboration Server and is welcomed by the IVR Welcome slide and message: Please enter the destination number followed by the dial tone.

Using the endpoint's DTMF input device such as remote control, the participant enters the number of the destination endpoint followed by the # key. Only one number can be dialed.

While the system dials to the destination endpoints, the participant hears the dialing rings. During the connection phase, the number being dialed is displayed on the screen of the calling endpoint.

If the call is not answered or it cannot be completed using one communication protocol, the system will try to connect the endpoint using the next communication protocol according to the selected protocols in the following order: H.323, SIP and ISDN.

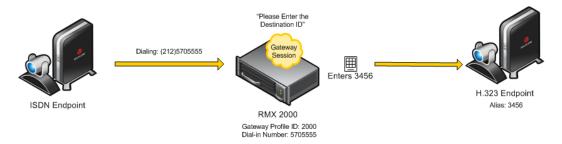
PSTN numbers are identified separately and are dialed immediately without trying other connections.

If the endpoint is busy, the system will not try to connect the endpoint using another protocol.

If the call is not completed after trying all possible protocols, the system displays the number that was dialed on the calling endpoint's screen and the reason for not completing the call. For details, see Connection Indications.

Dialing from ISDN/PSTN Endpoints

Dialing String and Call Flow from ISDN Endpoint to IP Endpoint



[GW Profile ISDN/PSTN number] - The dial-in number assigned to the Gateway Profile, including the required country and area codes.

For example, if the dial-in number assigned to the Gateway Profile is 5705555, enter this number with the appropriate area code: 2125705555.

Once the participant is connected to the Gateway Profile and hears the IVR message requesting the destination number, using the DTMF input keypad, the participant enters the number of the destination endpoint followed by the # key. For example, enter 3456# for IP endpoint.

To enter an IP address as the destination number, replace the periods (.) with asterisks (*) in the format n*n*n*n followed by the # key. For example, if the IP address is 172.22.188.22, enter 172*22*188*22#.

PSTN Dial-in Using GK Prefix

When connecting to an Collaboration Server that is standalone or part of a DMA solution deployment, PSTN participants are prompted by an IVR message requesting the **Destination Conference ID** followed by the # key to be entered using the DTMF input keypad.

Including the Gatekeeper Prefix in the DTMF input string enables PSTN participants to use the input string when connecting to an Collaboration Server whether the Collaboration Server is a standalone MCU or part of a DMA solution deployment. For a detailed description, see PSTN Dial-in Using GK Prefix.

Direct Dial-in to Endpoints or DMA VMR using Automatically Generated Destination Numbers

ISDN/PSTN participants can call the destination endpoints without interaction with the IVR of the gateway. This dialing method is enabled when the administrator configures the Gateway Profile to automatically generate the dial string of the destination endpoint or Meeting Room on the DMA by truncating the dial in string and replacing the truncated digits by other digits that can be used as the destination number.

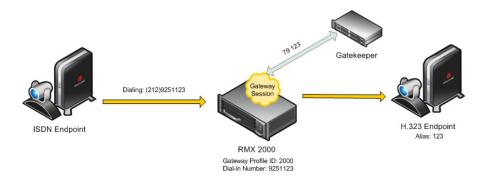
For a detailed description of the call flow when dialing the DMA using this method, see Calling a RealPresence DMA Direct with Automatically Generated Destination Dial Strings.

Calling an IP Endpoint via Gateway

If the call destination is an IP endpoint, the endpoints must be registered to the same gatekeeper to which the Collaboration Server is registered. There should be a mapping between the dial-in numbers in the range defined for the ISDN Network Service and also assigned to the Gateway Profile and the IP endpoints, in such a way that the alias of each endpoint is the number that will be appended to the ISDN prefix.

When the call arrives to the gateway, this prefix is truncated and replaced by digits that correspond to the MCU prefix in the gatekeeper and the call is forwarded to the destination endpoint.

Call Flow from ISDN Endpoint to H.323 Endpoint with Automatically Generated Forwarded Dial String



For example:

- The ISDN prefix is 9251.
- The dial in number range defined in the ISDN Network Service can be 100 to 400 (that is, 9251100 to 9251400).
- The dial in numbers assigned to the Gateway Profile can the entire range, or part of the range of other Gateway Profiles are to be used: 100 to 200 (that is 9251100 to 9251200).
- The aliases assigned to the IP endpoints will range between 100 to 200 or 400 (for the full range) as well.
- MCU Prefix in the gatekeeper: 79.
- Number of digits to append (same as the ISDN prefix is this example): 3.
- The destination endpoint alias is 123.
- The ISDN endpoint dials 9251123. The Collaboration Server truncates the four first digits 9251 replacing them with 79 and appends 123 to 79, to create the destination number 79123 which is sent to the gatekeeper for routing.

Interoperability with CMA

The Collaboration Server does not register to the gatekeeper as a Gateway, therefore it is recommended to create and use the CMA/DMA Dialing Rules to enable the CMA/DMA Dial One Method.

When the caller enters the Dial One digit as the destination number prefix, the CMA/DMA replaces this digit with the MCU prefix in the Gatekeeper and the ID of the Gateway Profile. For example, the calling participant can enter 99251444, where 9 is the digit that is used as the MCU prefix registered in gatekeeper and is replaced by the gatekeeper with * and the Gateway Profile ID (for example, *2000) as defined in the Dialing Rule.

For more details on Dialing Rules definition in the CMA/DMA, see the *Polycom CMA System Operations Guide*, "Dial Rule Operations" or the *Polycom RealPresence DMA System Operations Guide*, "Dial Rule Operations".

Configuring the Gateway Components on the Collaboration Server

To enable gateway calls in the Collaboration Server, the following components have to be configured:

- Conference IVR Service to be used with the Conference Profile assigned to the Gateway Profile. The IVR Services are used for Gateway IVR connections.
- Conference Profile that includes the IVR Service for the Gateway Session and the settings to automatically terminate the Gateway Session when one participant is still connected or when no participants are connected
- Gateway Profile for call routing.

Defining the IVR Service for Gateway Calls

The system is shipped with a default Conference IVR Services for gateway calls named GW IVR Service that enables you to run gateway calls without defining a new Conference IVR Service. This IVR Service includes the following settings:

- Welcome slide and message disabled
- Conference and Chairperson Passwords disabled
- General Messages all messages including the gateway messages and dial tones are selected
- Roll Call disabled
- Video Services Click&View enabled
- Video Services Video Welcome Slide Default_GW_Welcom_Slide
- Operator Assistance disabled

You can define a new Conference IVR Service to be used for gateway calls. This Conference IVR Service will be assigned to the appropriate Gateway Profile.

To define a new Conference IVR Service for gateway calls:

- 1 In the RMX Management Rarely Used pane, click the IVR Services (iii) entry.
 The list pane displays the Conference IVR Services list.
- 2 On the IVR Services toolbar, click **New Conference IVR Service** (**).
 - The New Conference IVR Service Global dialog box opens.
- 3 In the Conference IVR Service Name field, enter a name that will identify this service as a gateway IVR service.
- 4 Define the IVR Service Global parameters (it is recommended to use the system defaults). For more details, see Conference IVR Service Properties Global Parameters.
- 5 When defining a gateway IVR Service, the following options should remain disabled:
 - Welcome Messages (in the Conference IVR Service Welcome dialog box).
 - Chairperson Messages (in the Conference IVR Service Conference Chairperson dialog box).
 - > Password Messages (in the Conference IVR Service Conference Password dialog box)

6 Click the General tab.

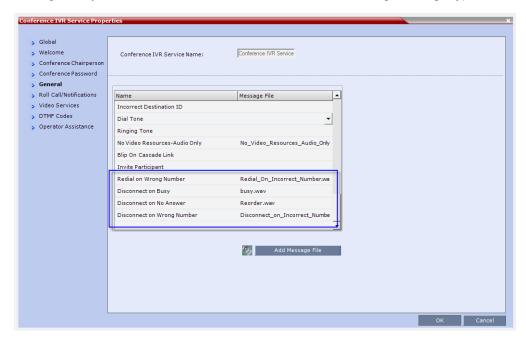
The **General** dialog box lists messages that are played during the conference. These messages are played when participants or the conference chairperson perform various operations or when a change occurs.

7 To assign the appropriate audio file to the message type, click the appropriate table entry, in the Message File column. A drop-down list is enabled.



For gateway redial, ensure that the audio files for the gateway redial messages have been assigned.

- 8 From the list, select the audio file to be assigned to the event/indication.
- **9** Repeat steps 7 and 8 to select the audio files for the required messages.
- 10 For a gateway IVR Service, select the audio file for the following message types:



Conference IVR Service Properties - Gateway General Voice Messages

Message Type	Description
Enter Destination ID	Prompts the calling participant for the destination number. Default message prompts the participant for the conference ID (same message as in the Entry Queue IVR Service).
Incorrect Destination ID	If the participant entered an incorrect conference ID (in gateway calls it is the destination number), requests the participant to enter the number again.
Dial Tone	The tone that will be played to indicate a dialing tone, to let the calling participant enter the destination number.

Conference IVR Service Properties - Gateway General Voice Messages

Message Type	Description
Ringing Tone	The tone that will be played to indicate that the system is calling the destination number.
Redial on Wrong Number	The message played when the wrong destination is entered, allowing you to enter a new number. For details, see Redial on Wrong Number.
Disconnect on Wrong Number	The message played when the wrong destination is entered, followed by a disconnection tone. For details, see Disconnect on Wrong Number.
Disconnect on Busy	The tone (or message) played when the dialed destination number is busy. For details, see Disconnect on Busy.
Disconnect on No Answer	The tone (or message) played when the dialed destination number does not answer. For details, see Disconnect on No Answer

- 11 When defining a gateway IVR Service, it is recommended that the **Roll Call** option remains disabled.
- 12 Click the Video Services tab.

The New Conference IVR Service - Video Services dialog box opens.

13 Define the following parameters:

New Conference IVR Service Properties - Video Services Parameters

Video Services	Description
Click&View	Select this option to enable endpoints to run the Click&View application that enables participants to select a video layout from their endpoint.
Video Welcome Slide	Select the video slide file to be displayed when participants connect to the conference. To view any slide, click the Preview Slide () button. If the video slide file was not uploaded to the MCU prior to the IVR Service definition, click the Add Slide button. The Install File dialog box opens. The uploading process is similar to the uploading of audio files. For more information, see step 7. Notes: • When using one of the default Polycom slides, the slide will be displayed in the resolution defined in the profile, i.e. CIF, SD, HD 720p or HD 1080p. • When defining a gateway IVR Service, the recommended default slide is: Default_GW_Welcome_Slide .

14 Click the **DTMF Codes** tab.

The New Conference IVR Service - DTMF Codes dialog box opens.

- **15** If required, modify the DTMF codes or permissions. For more details see New Conference IVR Service Properties DTMF Codes.
- 16 Click the Operator Assistance tab.
- **17** If Operator Assistance will not be available to participants, clear the **Enable Operator Assistance** option, which is automatically selected to disable it.

18 Click **OK** to complete the IVR Service definition.

The new Conference IVR Service is added to the IVR Services list.

Defining the Conference Profile for Gateway Calls

The Conference Profile that will be later assigned to the Gateway Profile determine the parameters of the gateway call, such as the line rate and video resolution and if to automatically terminate the gateway session when one participant or no participants are connected to the Gateway Session.

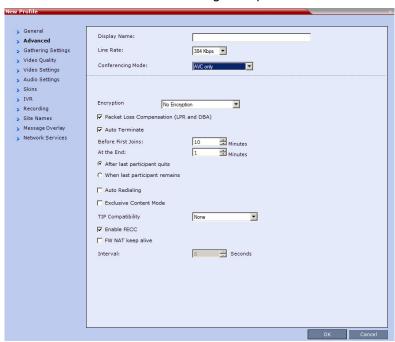


From Version 7.2, Gathering phase is not supported in gateway calls, even if it is defined in the Profile assigned to the Gateway Profile.

To define a Conference Profile for Gateway Sessions:

- 1 In the RMX Management Rarely Used pane, click Conference Profiles.
- 2 In the Conference Profiles pane, click New Profile.
 - The **New Profile General** dialog box opens.
- 3 Define the Profile name and select the line rate for the gateway session.
- 4 Click the Advanced tab.

The **New Profile – Advanced** dialog box opens.



- 5 Define the required settings for **Encryption** and **LPR**.
- 6 Set the **Auto Terminate At the End** option to **When Last Participant Remains** ensuring that the gateway call will end when only one participant is connected. For more details, see New AVC CP Profile Advanced Parameters.
- 7 Define the remaining Profile parameters as described in Defining AVC CP Conferencing Profiles.

Defining the Gateway Profile

A Gateway Profile is a conferencing entity, based on the Conference Profile assigned to it, that enables endpoints to dial-in and initiate Gateway Sessions. The system is shipped with a default Gateway Profile, named **Default_GW_Session**.

When an endpoint calls the Gateway Profile, a new Gateway Session is automatically created based on the Profile parameters, and the endpoint joins the gateway call which can also be a multipoint conference if more than two participants are connected to the conference.

The Gateway Profile defines the parameters of the gateway call that are taken from the Conference Profile assigned to it, such as line rate, resolution, the IVR Service to be used and the dial-in numbers.

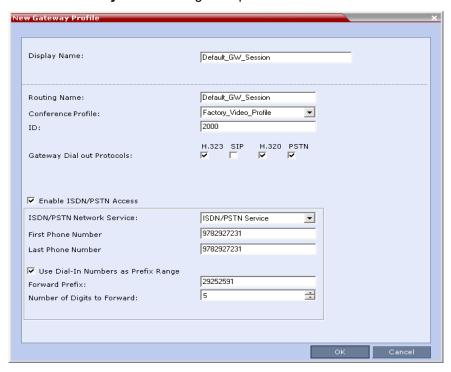


Up to 1000 Gateway Profiles, Entry Queues, IP Factories and Meeting Rooms can be defined in the Collaboration Server (they are all part of one repository whose size is 1000 entries).

To define a new Gateway Profile:

- 1 In the RMX Management Rarely Used pane, click Gateway Profiles =.
- 2 In the Gateway Profiles list pane, click the New Gateway Profile button.

 The New Gateway Profile dialog box opens.





Do not enable PSTN/ISDN access without defining the dial-in numbers range and/or the use of "Dial-In Numbers as Prefix Range". If you enable the PSTN/ISDN access without the definition of the dialing parameters, people can dial in to the gateway from outside the organization and then make long distance calls at the 'host' expense.

The new Gateway Profile is added to the list.

System Configuration

For details about adding and modifying system flags, see Manually Adding and Deleting System Flags.

Displaying the Connection Information

You can hide the connection indications displayed on the participant's screen during the connection phase by changing the system configuration and manually adding and setting the system flag **DISABLE_GW_OVERLAY_INDICATION** to **YES** in the **MCMS_PARAMETERS_USER** tab.

By default, this flag is set to NO and all connection indications are displayed.

Enabling PSTN dial-in using GK prefix

The feature is enabled when setting the flag USE_GK_PREFIX_FOR_PSTN_CALLS to Yes.

For more details, see PSTN Dial-in Using GK Prefix.

Gateway Calls Redialing

The Gateway can redial to numbers that are wrong, or busy or there is no answer.

Gateway Redial Guidelines

- Redial with IVR is supported:
 - > In CP environments only.
 - > For H.323, SIP and ISDN calls.
 - When using the Collaboration Server's Inviting Participants using DTMF functionality.
- Redial with IVR is not supported:
 - When using PCM's Invite Participant functionality.
 - Dialing multiple destination numbers.

Redial on Wrong Number

An IVR message is played requesting the user to enter a new number, followed by up to five redial attempts. If all redial attempts fail, the user is alerted by an IVR message that the dialed number is unreachable, followed by reorder tone and disconnection.

Wrong Destination Number

 The number of re-dial attempts is controlled by the WRONG_NUMBER_DIAL_RETRIES system flag.

The default number of redial attempts is **3**. To modify the number of redial attempts, manually add the flag to *system.cfg* and set its value to the number of redial attempts required.

The flag value range is **0-5**. A flag value of **0** means that no redials are attempted.

For more information about system flags see Manually Adding and Deleting System Flags.

- Redial attempts follow the same order as defined in the Gateway Profile: H.323, followed by SIP, followed by ISDN. For more information about Gateway Profiles and Gateway Dial out Protocols see Defining the Gateway Profile.
- Redial on Wrong Number is activated if a Gateway Call fails, for all defined protocols, for any reason or combination of reasons listed in the following table.

Call Failure Reasons - H.323, SIP, ISDN

H.323	SIP	ISDN
Unreachable Destination	484 - Address Incomplete	3 - No Route to Destination
Bad Format Address	404 - Not Found	18 - No User Responding
Adaptive Busy	414 - Request-URI Too Long	28 - Invalid Number Format
Admission Rejected (ARJ) Reason: Request Denied Item 1: Cannot find location.	416 - Unsupported URI Scheme	41 - Temporary Failure
Admission Rejected (ARJ) Reason: Called Party Not Registered	420 - Bad Extension	
	421 - Extension Required	

The user receives the Redial on Wrong Number IVR message: Incorrect destination. Please enter the destination number.

If all the redial attempts fail the user receives the Disconnect on Wrong Number IVR message: Destination could not be reached; call is disconnected.

 Gateway Re-dial is not activated if the reason for call failure is Busy or No Answer, for any of the defined protocols.

Wrong Destination Number Time-out

- A time-out counter is started when the Redial on Wrong Number message is played. If the user does
 not enter another destination number within the time-out period it is considered a failed dial out
 attempt.
- The Redial on Wrong Number message and time-out are repeated according to the value of the WRONG_NUMBER_DIAL_RETRIES system flag. If there is no input from the user, after completing the retries, the user receives the Disconnect on Wrong Number IVR message: Incorrect destination number followed by the Reorder Tone.

Disconnect on Busy

Redialing of calls to busy destination can be selected. The number of redial attempts is dependent on the **NUMBER_OF_REDIAL** system flag, the default value is **3**.

If all redialing retry attempts fail, the user receives the Disconnect on Busy message in the form of Busy Tone. The call is then disconnected.

Disconnect on No Answer

If all retry attempts fail, the user receives the Disconnect on No Answer message in the form of Reorder Tone. The call is then disconnected.

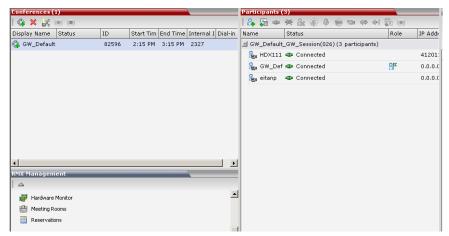
Disconnect on Wrong Number

In previous versions, if a call failed due to no answer at the destination, the call was disconnected with no notification.

When using this version, the user receives the Disconnect on Wrong Number IVR message: **Incorrect Destination Number** followed by **Reorder Tone**. The call is then disconnected.

Monitoring Ongoing Gateway Sessions

Ongoing Gateway Sessions that are created when calling the Gateway Profile, are listed in the ongoing Conferences list pane.



Gateway Sessions are monitored in the same way as the conferences. For more details on monitoring conferences, see Conference Level Monitoring.



Additional ISDN and PSTN Participants cannot dial in directly to the Gateway Session once it was started.

Connection Indications

During the connection process to the other endpoints, the system displays on the calling participant's screen the called number and the connection status.

A Maximum of 32 characters can be displayed for connection indications. If the displayed information is longer than 32 characters the text is truncated.

If the system dials out to only one destination endpoint, the dialed number is not shown, only the connection status.

If the destination endpoint is ISDN, the system displays the connection progress in percentages, where the percentages represent various stages in the connection process as follows:

- Up to 60% the connection of the ISDN channels (up to 30 channels can be connected when E1 is used for the connection).
- 60% 80% BONDING stage.
- 80% 90% Capability exchange stage.
- 90% 99% Media connection stage.

Once the call is completed, the indications are cleared.

If the call is not completed after trying all possible protocols, the system displays the number that was dialed on the calling endpoint's screen and one of the following causes:

- **Busy** The far endpoint is in another call. In such a case, the system does not try to connect using another communication protocol.
- Rejected The far endpoint has rejected the call. In such a case, the system will try to connect using another communication protocol.
- Unreached The number could not be resolved by the gatekeeper or the SIP proxy or could not be found on the network. In such a case, the system will try to connect using another communication protocol.
- **Failed** Any reason causing the system not to complete the connection process. In such a case, the system will try to connect using another communication protocol.

You can hide the connection indications by changing the system configuration. For more details, see System Configuration.

Gateway Session Parameters

The Collaboration Server creates a new conference that acts as a Gateway Session.

Gateway Session Name

The Gateway Session has a unique ID whose display name is composed of the following components:

- The prefix GW ,
- The Gateway Profile display name. For example, Default GW Session
- (number) where the number is a gateway conference counter.

For example: if the Gateway Profile display name is Default_GW_Session, the conference name will be GW_Default_GW_Session(001).

Conference ID

The ID of the new conference is assigned randomly by the MCU.

The Gateway Session automatically ends when only one participant is left in the session.

Connected Participant Parameters

Once this conference is created, the calling participant is connected to it and one or several dial-out participant(s) are automatically created and added to this gateway session. The dial-in participant is also identified as the chairperson of the conference.

The connecting (dial-in) participant name is taken from the endpoint. If the endpoint does not send its name, it is derived from the Gateway Profile display name and it includes the Gateway Session name, underscore and a random number is displayed (between brackets), for example,

```
GW Default GW Session(001) (000).
```

The name of the destination (dial-out) participant is taken from the endpoint. If the endpoint does not send its name, it is taken from the dialed number. If the dialed number was an IP address, the system displays underscores instead of dots, for example, 172 22 172 89.

Participants connected to a gateway session are monitored in the same way as participants connected to ongoing conferences. For details, see Participant Level Monitoring.

Direct Dialing from ISDN/PSTN Endpoint to IP Endpoint via a Meeting Room

Dialing from an ISDN endpoint to a specific IP endpoint using the Gateway Profile is a two-step process (dialing to the Gateway and then entering the number of the destination IP endpoint).

When dialing to specific IP endpoints you can simplify the dialing process by creating the appropriate Meeting Room.

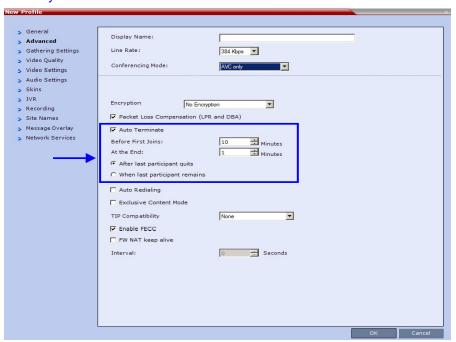
If CMA is involved, dialing can be simplified even further by configuring the appropriate dialing Rule in the CMA/DMA.

To set up the Meeting Room for direct dialing in:

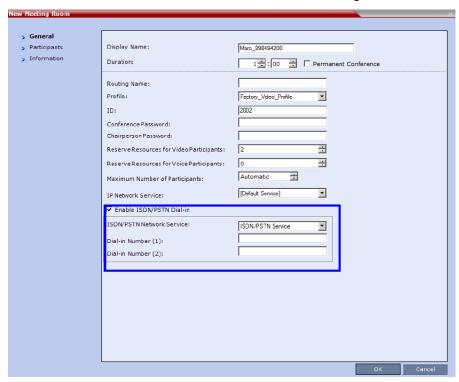
Set the conference parameters in the Conference Profile and make sure that the conference will automatically end when there is only one participant connected to the meeting.

Define the Meeting Room with the following:

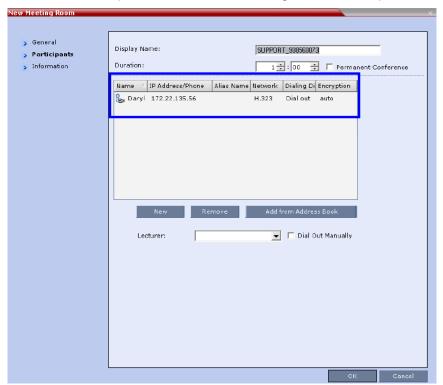
Conference Profile in which the Auto Terminate - At the end - When Last Participant Remains
option is selected. For more details on Conference Profile definition, see Defining the IVR Service for
Gateway Calls.



ISDN/PSTN access is enabled and a dial-in number is assigned to the Meeting Room.



• The dial-out IP endpoint is added to the Meeting Room's Participants list.



Dialing to Polycom® RealPresence DMA System

Two dialing methods are available to ISDN/PSTN participants calling the DMA:

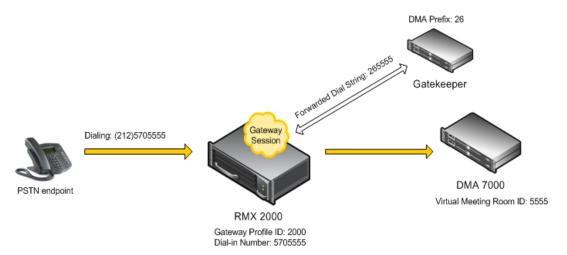
- Direct with automatically generated destination dial strings from dial-in strings. This option is available only from version 7.1 and only to Collaboration Server with MPM+ and MPMx cards.
- Via Gateway IVR.

In addition, PSTN participants can dial the Gateway IVR and can use the MCU or DMA prefix in the gatekeeper together with the conference ID/endpoint alias as the destination string to simplify the input. This is one of the methods for PSTN participants to connect to a virtual Meeting Room on the DMA. For more details, see PSTN Dial-in Using GK Prefix.

Calling a RealPresence DMA Direct with Automatically Generated Destination Dial Strings

In this configuration, the gateway session initiator enters one of the dial-in numbers assigned to the gateway profile. This number is truncated by the Collaboration Server gateway and the truncated digits are replaced by a prefix that corresponds either to the DMA prefix in the Gatekeeper.

Call Flow from ISDN Endpoint to Polycom DMA with Automatically Generated Forwarded Dial String



Example:

The figure above shows the call flow assuming the following parameters:

First Dial-in Number	5705550
Look Diel in Number	
Last Dial-in Number	5705560
Use Dial-in Numbers as Destination ID	Selected
DMA Meeting Room ID	5555
Destination Prefix (DMA prefix in Gatekeeper)	26
Number of Rightmost Digits to Append 4	

PSTN participant dials	(212)5705555
Number that will be used by Collaboration Server to forward the call to the DMA	265555

Calling the RealPresence DMA via Gateway IVR

Audio PSTN/ISDN calls can be routed to Polycom DMA 7000 via the Collaboration Server. ISDN Video endpoints connect using their audio channels (but consume video resources). The RealPresence DMA system enables load balancing and the distribution of multipoint calls on up to 10 Polycom Collaboration Server media servers.

As part of this solution, the Collaboration Server acts as a gateway for the DMA that supports H.323 calls. The PSTN or ISDN endpoint dials the virtual Meeting Room on the DMA via the Gateway Profile on the Collaboration Server.

Both the Collaboration Server and the RealPresence DMA must be registered with the same gatekeeper.

The dialing string of the destination conference on the RealPresence DMA must be communicated to the dialing endpoint and used during the connection to the Gateway Profile on the Collaboration Server. There are two options available for doing this:

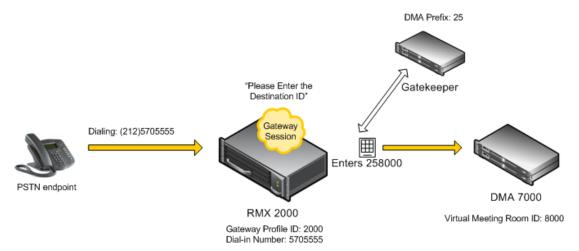
- Manual Dial String Entry
- · Automatic Dial String Generation

Manual Dial String Entry

Dialing String and Call Flow from ISDN Endpoint to Polycom DMA

The connection is done in two steps:

- A PSTN/ISDN participant dials the dial-in number assigned to the Gateway Profile (5705555), including the country and area code (if needed) and connects to the Gateway IVR.
- When prompted for the target conference ID, the caller enters the string of the target meeting room on the DMA followed by the # key.



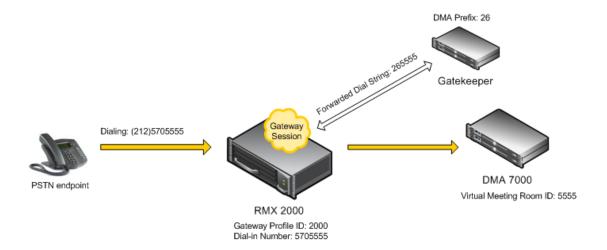
This string is composed of the RealPresence DMA prefix as registered in the gatekeeper and the ID of the virtual meeting room running on the RealPresence DMA. For example, if the DMA prefix is 25 and the target meeting room ID is 8000 the participant enters 258000 followed by the # key.

The Collaboration Server creates a Gateway Session with two participants, the calling participant and the link to the conference running on the RealPresence DMA.

Automatic Dial String Generation

The administrator can configure the Gateway Profile to automatically generate and forward the dial string from the Collaboration Server Gateway Session to the RealPresence DMA in order to connect to the required RealPresence DMA Meeting Room. When this configuration option is selected, the participant does not need to interact with the IVR Service.

Call Flow from ISDN Endpoint to RealPresence DMA with Automatically Generated Forwarded Dial String



Example:

The figure above shows the call flow assuming the following parameters:

First Dial-in Number	5705550
Last Dial-in Number	5705560
Use Dial-in Numbers as Destination ID	Selected
DMA Meeting Room ID	5555
Destination Prefix (DMA Gatekeeper)	26
Number of Rightmost Digits to Append	4
PSTN participant dials	(212)5705555

PSTN Dial-in Using GK Prefix

When connecting to an Collaboration Server that is standalone or part of a DMA solution deployment, PSTN participants are prompted by an IVR message requesting the Destination Conference ID followed by the # key to be entered using the DTMF input keypad.

Including the Gatekeeper Prefix in the DTMF input string enables PSTN participants to use the input string when connecting to an Collaboration Server whether the Collaboration Server is a standalone MCU or part of a DMA solution deployment.

Enabling PSTN dial-in using GK prefix

The feature is enabled by the **USE_GK_PREFIX_FOR_PSTN_CALLS** system flag in system.cfg. For more information see Modifying System Flags.

The following table summarizes the PSTN participant's DTMF input depending on the flag value.

PSTN Participant input via DTMF

	FLAG: USE_GK_PREFIX_FOR_PSTN_CALLS=	
Configuration	NO	YES
Standalone Collaboration Server Conference ID= 1234	PSTN participant enters: 1234# .	PSTN participant enters: 761234#
Collaboration Server with DMA Virtual Meeting Room ID in DMA = 1234 DMA gatekeeper prefix = 76	PSTN participant enters: 761234#	 (The Gatekeeper Prefix"76" is automatically removed from the DTMF input string for a standalone Collaboration Server.)

Deploying a Polycom RMX™ Serial Gateway S4GW

UC APL Public Key Infrastructure (PKI) requires that the Serial Gateway S4GW be connected directly to the Collaboration Server and not to the H.323 network. The Serial Gateway effectively becomes an additional module of the Collaboration Server, with all web and H.323 traffic passing through the Collaboration Server.

For more information see the *RealPresence Collaboration Server* (*RMX*)1500/2000/4000 Deployment Guide for Maximum Security Environments, Deploying a Polycom RMX™ Serial Gateway S4GW.

RMX Manager Application

The RMX Manager is the Windows version of the Collaboration Server Web Client. It can be used instead of the Collaboration Server Web Client for routine Collaboration Server management and for Collaboration Server management via a modem connection. For more information on using the RMX Manager via a modem connection, see Appendix G - Configuring Direct Connections to the Collaboration Server.



For Maximum Security Environments, the RMX Manager is the recommended option for accessing the RMX's management console. The RMX Manager specific to the Maximum Security version being deployed can be downloaded from the Support section of the Polycom website.



Modem connection is not supported when the Collaboration Server is in Ultra Secure Mode. For more information see Ultra Secure Mode.

Using the RMX Manager application, a single user can control a single or multiple MCU units as well as conferences from multiple MCUs. The RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 system can be managed and controlled by the RMX Manager application.

The RMX Manager can list and monitor:

- Up to 20 Collaboration Server systems in the MCUs pane
- Up to 800 conferences in the Conferences pane
- Up to 1600 participants in the Participants pane

The RMX Manager is faster than the RMX Web Client and can give added efficiency to Collaboration Server management tasks, especially when deployed on workstations affected by:

- Lack of performance due to bandwidth constraints within the LAN/WAN environment.
- Slow operation and disconnections that can be caused by the anti-phishing component of various antivirus applications.



Users with **Auditor** authorization level cannot connect to the RealPresence Collaboration Server via the RMX Manager application and must use the RMX Web Client.

The RMX Manager application can be installed in your local workstation or accessed directly on the RealPresence Collaboration Server system without installing it in your workstation.

Installing the RMX Manager Application

The installation of the RMX Manager Application includes two main stages:

- Accessing or downloading the RMX Manager Installer
- INstalling the RMX Manager application



For information about Installing the RMX Manager for Secure Communication Mode see the RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide for Maximum Security Environments, Download and Install the RMX Manager Onto a Workstation.



Upgrade Notes

- When upgrading the RMX Manager application, it is recommended to backup the MCU list using the Export RMX Manager Configuration option. For more details, see Import/Export RMX Manager Configuration.
- When upgrading the RMX Manager from a major version (for example, version 8.7.0) to a
 maintenance version of that version (for example, 8.7.0.x), the installation must be performed from
 the same MCU (IP address) from which the major version (for example, version 8.7.0) was
 installed.

If you are upgrading from another MCU (different IP address), you must first uninstall the RMX Manager application using **Control Panel > Add or Remove Programs**.



New RealPresence Collaboration Server Installation Note

When managing the RealPresence Collaboration Server, upgrade/install the latest MCU version and then install the latest RMX Manager application.

The Collaboration Server Installation and First Entry Configuration must be completed before installing the RMX Manager application. For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Software Installation.

Once the connection to the Collaboration Server unit is established and the Login window is displayed, the RMX Manager application can be installed.

Accessing or downloading the RMX Manager Installer

The RMX Manager installer can be downloaded or accessed and installed on your workstations using one of the following methods:

- Accessing the RMX Manager Application Installer Directly from the MCU
- Downloading the RMX Manager application from the Polycom web site at http://www.polycom.com/support and installing it. The Installation procedure is the same as if you have downloaded the application from the Login screen.
- Accessing the RMX Manager Installer from the Login screen

Accessing the RMX Manager Application Installer Directly from the MCU

1 Start Internet Explorer and in your browser enter:

http://<Collaboration Server IP Address>/RMXManager.html.

For example, if the Collaboration Server IP address is 10.226.10.46, enter in the browser the following address: http://10.226.10.46/RMXManager.html.

The RMX Manager Version nnnn page is displayed.

2 Click Install.



The installer verifies the application's requirements on the workstation.



3 Continue the Installation as described in Installing the RMX Manager on Your Workstation.

Downloading the Installation files from Polycom Support Site

- 1 Access the Polycom web site at http://www.polycom.com/support.
- 2 Click on Documents and Downloads and then select UC Infrastructure from the drop-down list
- 3 Select the appropriate RMX/Collaboration Server product.
- 4 Click the RMX 1500/2000/4000 version n.n.n.n Local Web Client (RMX Manager) link. The file download dialog box opens.
- 5 Follow the standard download procedure to either run the installer directly or save the files to your local computer.
- 6 Continue the Installation as described in Installing the RMX Manager on Your Workstation.

Accessing the RMX Manager Installer from the Login screen

1 Start Internet Explorer and connect to one of the Collaboration Server units in your site. It is recommended to connect to the Collaboration Server installed with the latest software version.

The **Login** screen is displayed.

There is a link to the **RMX Manager Installer** at the top of the right edge of the screen.



2 Click the Install RMX Manager link.

The installer verifies the application's requirements on the workstation.



The **Install** dialog box is displayed.

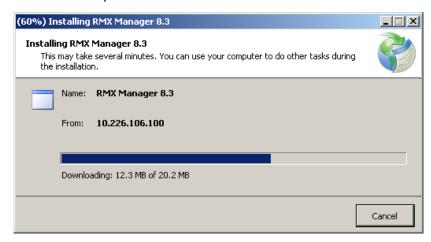
Installing the RMX Manager on Your Workstation

Once the installer has verified that the application's requirements on the workstation are met, the The **Install** dialog box is displayed.

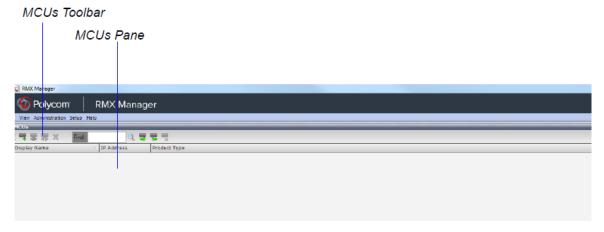
Click the Install button.



The installation proceeds.



The installation completes, the application loads and the RMX Manager - MCUs screen is displayed.



The first time you start the RMX Manager application, the **MCUs** pane is empty.

Starting the RMX Manager Application

Once installed, the RMX Manager can be run using the http:// (non-secured) or https:// (secured) command in the browser's address line or the Windows **Start** menu.

To use the browser:

1 In the browser's command line, enter:

```
http://<MCU Control Unit IP Address>/RMXManager.html
or
https://<MCU Control Unit IP Address>/RMXManager.html
```

2 Press Enter.

To use the Windows Start menu:

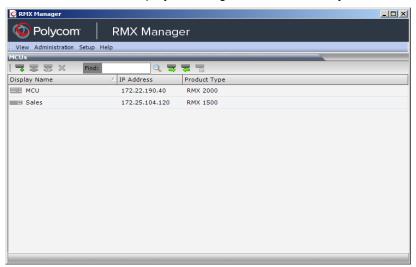
- 1 Click Start > Programs.
 - **a** If the RMX Manager is displayed in the recently used programs list, click **RMX Manager** in the list to start the application.

or

b Click All Programs > Polycom > RMX Manager.



The MCUs screen is displayed, listing the MCUs currently defined in the RMX Manager.



This screen enables you to add additional MCUs or connect to any of the MCUs listed. For details on adding MCUs, see Adding MCUs to the MCUs List.

For each listed MCU, the system displays the following information:

- MCU Display Name (as defined in the Add MCU dialog box).
- > IP Address of the MCU's control unit
- ➤ **Product Type** The MCU type: RealPresence Collaboration Server 800s, RMX VE, RealPresence Collaboration Server (RMX) 1500, RealPresence Collaboration Server (RMX) 2000, or RealPresence Collaboration Server (RMX) 4000.

Before connecting to the MCU for the first time, the Collaboration Server type is unknown so **RMX** is displayed instead as a general indication.

To display the RMX Manager main screen you must connect to one of the listed Collaboration Servers. For more details, see Connecting to the MCU.

Connecting to the MCU

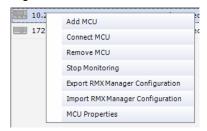
Once an MCU is defined, the RMX Manager can be connected to it. This allows you to set up conferences, make reservations, monitor On Going Conferences and perform other activities on several MCUs.



The first Collaboration Server unit that is connected to the RMX Manager dictates the Authorization Level of Users that can connect to the other MCUs on the list. For example, if the Authorization level of the User POLYCOM is Administrator, all Users connecting to the other MCUs on the list must be Administrators. Each user can have a different login name and password for each of the listed MCUs and they must be defined in the Users list of each of the listed MCUs.

To connect the RMX Manager to an MCU:

- 1 In the **MCUs** pane or screen, use one of the following methods:
 - a Double-click the MCU icon.
 - **b** Select the Collaboration Server to connect and click the **Connect MCU** when button.
 - c Right-click the MCU icon and then click Connect MCU.

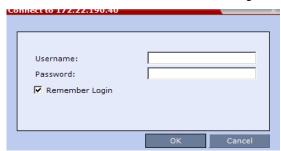


If you are connecting to the MCU from the MCUs opening screen and have defined the Username and Password for the connecting MCU, the system connects to the Collaboration Server, and the RMX Manager Main Screen is displayed.



If you are connecting to any MCU from the MCUs pane in the RMX Manager Main Screen and have defined the **Username** and **Password** for the connecting MCU, the MCU icon changes to connected and its status, type and number of audio and video resources are displayed in the MCUs pane.

If the Username and Password are missing from the MCU parameters, or if the **Remember Me** check box has been cleared, the **Connect** dialog box opens.



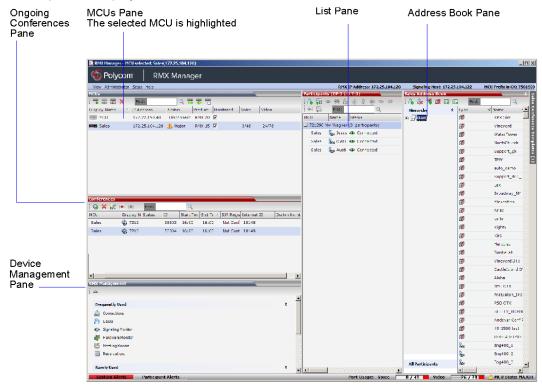
- 2 In the **Username** field, enter the user name with which you will login to the MCU.
- 3 In the **Password** field, enter the password as defined for the user name with which you will login to the MCU.
- 4 To add the user name and password to the MCU properties so you will not have to enter them each time you login to the MCU, make sure that the **Remember Login** check box is selected. Otherwise, clear the **Remember Login** check box.
- 5 Click OK.

The system connects to the Collaboration Server, and the RMX Manager Main Screen is displayed. If a User with the entered Username and Password is not defined in the Collaboration Server, an error message is displayed and the system lets you re-enter the Username and Password.

RMX Manager Main Screen

The RMX Manager Main Screen is displayed only when at least one MCU is connected.

This screen is similar to the RMX Web Client Main Screen with the addition of the **MCUs** pane. As in the RMX Web Client, the panes are displayed according to the Authorization Level of the logged in User. The **MCUs** pane is displayed to all users.

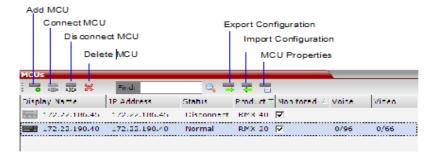


Only one MCU can be selected in the **MCUs** pane. If only one MCU is connected, it is automatically selected. The selected MCU is highlighted.

The menu items, the Collaboration Server Management features, the Address Book and the Conference Templates are all properties of the selected MCU and apply to it.

MCUs Pane

The **MCUs** pane includes a list of MCUs and a toolbar.



For each listed MCU, the system displays the following information:

MCU Display Name - the name of the MCU and its icon according to its type and connection status.
 The following icons are available:

MCU Icons and Statuses

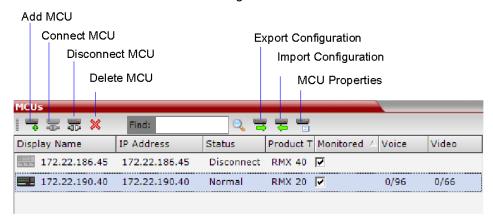
Icon	Description
	RealPresence Collaboration Server (RMX) 1500, disconnected.
	RealPresence Collaboration Server (RMX) 1500, connected.
	RealPresence Collaboration Server (RMX) 2000, disconnected.
	RealPresence Collaboration Server (RMX) 2000, connected.
	RealPresence Collaboration Server (RMX) 4000, disconnected.
	RealPresence Collaboration Server (RMX) 4000, connected.
	RealPresence Collaboration Server 1800, disconnected
	RealPresence Collaboration Server 1800, connected
	RealPresence Collaboration Server 800s, disconnected
	RealPresence Collaboration Server 800s, connected
	RealPresence Collaboration Server Virtual Edition, disconnected
	RealPresence Collaboration Server Virtual Edition, connected

- IP Address of the MCU's control unit.
- Status The status of the MCU:
 - Connected the MCU is connected to the RMX Manager and can be managed by the RMX Manager user.
 - Disconnected The MCU is disconnected from the RMX Manager
 - > Major The MCU has a major problem. MCU behavior could be affected and attention is required.
- Product Type The MCU type: RealPresence Collaboration Server 1500/2000/4000, RealPresence Collaboration Server 1800, RealPresence Collaboration Server 800s, RealPresence Collaboration Server Virtual Edition. Before connecting to the MCU for the first time, the Collaboration Server type is unknown so RMX is displayed instead as a general indication.
- Monitored When checked indicates that the conferences running on this MCU are automatically added to the Conferences list and monitored. To stop monitoring the conferences running on this MCU and their participants, clear the Monitored check box.
- Video Resources The number of video resources that are available for conferencing.

Audio Resources - The number of audio resources that are available for conferencing (applicable
to Collaboration Server 1500/2000/4000 in MPMx Card Configuration Mode only).

MCUs Toolbar

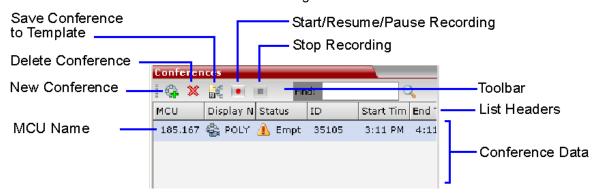
The **MCU** toolbar contains the following buttons:



Conferences Pane

The Conferences pane lists all the ongoing conferences from all the MCUs that are connected and monitored along with their MCU, Status, Conference ID, Start Time and End Time data. The number of ongoing conferences is displayed in the pane's title.

The **Conferences** list toolbar contains the following buttons:



If Conference Recording is enabled the following buttons are enabled:

- Start/Resume Recording Start/resume recording.
- Stop Recording Stop recording.
- Pause Toggles with the Start/Resume button.

Monitoring conferences

New conferences run on MCUs selected for Monitoring are automatically added to the **Conferences** list. You can sort the conferences by MCU by clicking the **MCU** column heading in the **Conferences** table. Conferences run on MCUs that are connected but not monitored are not listed.

Using Windows multiple selection methods to select conferences, participants from several conferences running on different MCUs can be listed in the **Participants** list pane.

Starting a new conference

When starting a new conference, you must first select the MCU to run the conference in the MCUs pane.

Collaboration Server Management

The Collaboration Server **Management** pane lists the entities of the selected MCU that need to be configured to enable the Collaboration Server to run conferences. Only users with Administrators permission can modify these parameters.

The Collaboration Server **Management** pane is divided into two sections:

- Frequently Used Parameters often configured monitored or modified.
- Rarely Used Parameters configured during initial system set-up and rarely modified afterward.

List Pane

The **List** pane displays details of the participants connected to the conferences selected in the **Conferences** pane or the item selected in Collaboration Server **Management** pane. The title of the pane changes according to the selected item.

When selecting an item in the Collaboration Server **Management** pane it applies only to the MCU selected in the MCUs list. In such a case, the system displays the name of the selected MCU in the List pane title.



Status Bar

The Status Bar at the bottom of the RMX Web Client contains System and Participant Alerts tabs as well as Port Usage Gauges and an MCU State indicator.

Status Bar - RealPresence Collaboration Server (RMX) 1500/2000/4000 With an MPMx Card

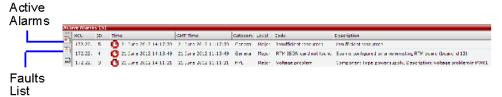


System Alerts

Lists system problems of all connected MCUs (even if the MCU is not monitored). The alert indicator flashes red when at least one system alert is active. The flashing continues until a user with Operator or Administrator permission reviews the list.

The System Alerts can be sorted by MCU by clicking the MCU header in the **System Alerts** table.

The **System Alerts** pane is opened and closed by clicking **System Alerts** in the left corner of the **Status** Bar.



For more information about Active Alarms and Faults List, see System and Participant Alerts.

Participant Alerts

Lists the participants of all monitored MCUs that are experiencing connection problems. The list is sorted by MCU and conference.

The Participant Alerts can be sorted by MCU by clicking the MCU header in the Participant Alerts table.

The Participant Alerts pane is opened and closed by clicking **Participant Alerts** in the left corner of the Status Bar.



Port Usage Gauges

In the RealPresence Collaboration Server (RMX) 1500/2000/4000, the **Port Usage** gauges displays for the selected MCU:

- The total number of Video or Voice ports in the system according to the Video/Voice Port
 Configuration. The Audio gauge is displayed only if Audio ports were allocated by the administrator,
 otherwise only the Video port gauge is displayed.
- The number of Video and Voice ports in use.
- The High Port Usage threshold.

In the RealPresence Collaboration Server 1800 and the RealPresence Collaboration Server (RMX) 2000/4000 with MPMRx card, the Port Usage Gauge displays for the selected MCU:

- The total number of Video ports in the system.
- The number of Video ports in use.
- The High Port Usage threshold.

For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Port Usage Gauges.

MCU State

The MCU State indicator displays the status of the selected MCU.

For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, MCU State.

Address Book

Displays the Address Book of the selected MCU (regardless of its Monitored status). The Address Book is a list of Participants and Groups that have been defined on the selected Collaboration Server.

The information in the Address Book can be modified only by an administrator. All Collaboration Server users can, however, view and use the Address Book to assign participants to conferences.

The name of the selected Collaboration Server is displayed in the title of the **Address Book** pane. For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Address Book.

Conference Templates

Conference Templates enable administrators and operators to create, save, schedule and activate identical conferences.

The Conference Templates pane lists the Conference Templates that have been defined on the selected Collaboration Server (regardless of its Monitored status).

The Conference Templates pane is initially displayed as a closed tab. The name of the selected Collaboration Server and the number of saved Conference Templates is indicated on the tab.

For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Conference Templates.

Adding MCUs to the MCUs List

The RMX Manager can connect to one or several Collaboration Servers simultaneously. If the site's configuration includes more than one MCU, or when a new MCU is added to your configuration, and you want to monitor and control all MCUs from within the same window, you must add the MCU to the MCUs list.



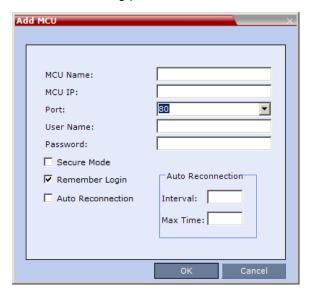
The Collaboration Server must be installed and its IP addresses properly configured in the Management Network Service before defining its connection parameters in the RMX Manager application.

To add the MCU to the list of MCUs being managed, define the MCU's connection parameters.

To add a Collaboration Server unit:

1 On the MCUs toolbar, click Add MCU • to add an MCU to the MCU list. The Add MCU dialog box opens.

2 Define the following parameters:



MCU Properties

Field	Description
MCU Name	Enter the name of the MCU on the network.
MCU IP	Enter the IP address of the MCU's Control Unit. The IP address must be identical to the one configured in the MCU during first entry Configuration.
Port	Enter the number of the port used for communication and data transactions between the Collaboration Server unit and the RMX Manager. For standard connection, enter 80. For a Secured connection (using TLS or SSL), enter 443.
Username	Enter the user name with which you will login to the MCU. A User with this name must be defined in the Collaboration Server Users list. The system is shipped with a default User whose name is POLYCOM.
Password	Enter the password as defined for the user name with which you will login to the MCU. The system is shipped with a default User whose password is POLYCOM.
Secure Mode	Optional . Select this check box to connect to the Collaboration Server with SSL and work in Secure Mode.
Remember Login	This check box is automatically selected, and it enables the usage of the user name and password entered in this dialog box when connecting to the Collaboration Server. If this check box is cleared, the user is prompted for the user name and password when connecting to this Collaboration Server unit.
Auto Reconnection	Select this check box to automatically reconnect to the Collaboration Server if the connection between the RMX Manager and the MCU is broken.

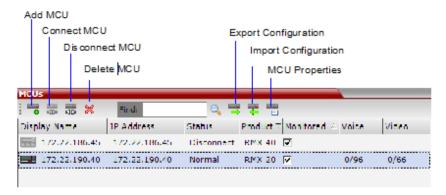
Field	Description
Interval	Enter time in seconds between reconnect ion attempts to the Collaboration Server. For example, if you enter 10, the system will wait 10 seconds between the connection attempts.
Max Time	Enter the maximum amount of time in seconds that the Collaboration Server is allowed to try to reconnect. If the Collaboration Server reconnects before the allotted time frame the count down timer is halted. For example, if you enter 100, the system will stop trying to reconnect if it has failed to do so within 100 seconds.

3 Click OK.

The MCU is added to the MCUs pane.

4 If required, repeat steps 1-3 to define additional Collaboration Server units.

The MCUs pane contains the list of all defined MCUs.



Starting a Conference

There are several ways to start a conference:

- Clicking New Conference in the Conferences pane. For more information, see Starting a Conference from the Conferences Pane.
- Dialing in to a Meeting Room defined on any of the MCUs.
 - ➤ A Meeting Room is a conference that is saved on the MCU. It remains in passive mode until it is activated by the first participant, or the meeting organizer dialing in. For more information about Meeting Rooms, see Meeting Rooms.
- Dialing in to an Ad Hoc Entry Queue defined on one of the MCUs which is used as the access point to the MCU.

For a detailed description of Ad Hoc Entry Queues, see Entry Queues.

- Start a Reservation:
 - If the Start Time of the Reservation is past due the conference becomes ongoing immediately.
 - > If the **Start Time** of the Reservation is in the future the conference becomes ongoing, at the specified time on the specified date.

For more information, see Starting a Reservation.

Start any Conference Template saved in the Conference Templates list.
 For more information, see Starting an Ongoing Conference or Reservation From a Template.

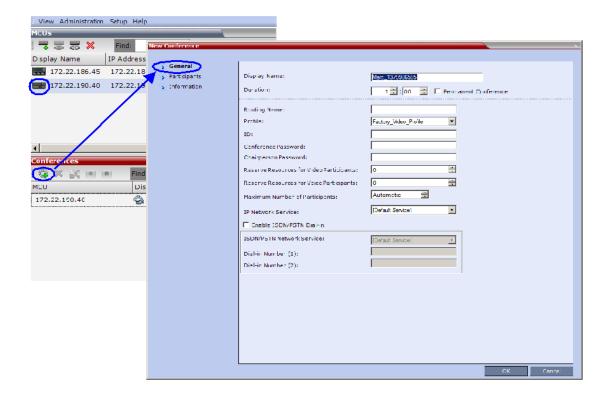
Starting a Conference from the Conferences Pane

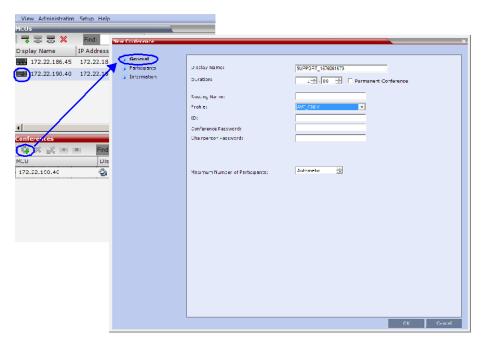
To start a conference from the Conference pane:

- 1 In the MCUs pane, select the MCU to run the conference.
- 2 In the Conferences pane, click the New Conference (4) button.

The New Conference - General dialog box opens.

RealPresence Collaboration Server (RMX) 1500/2000/4000 New Conference - General Dialog Box





RealPresence Collaboration Server 1800 New Conference - General Dialog Box

The system displays the conference's default Name, Duration and the default Profile, which contains the conference parameters and media settings.

The Collaboration Server automatically allocates the conference ID, when the conference starts.

In most cases, the default conference ID can be used and you can just click **OK** to launch the conference. If required, you can enter a conference ID before clicking **OK** to launch the conference.

If you are the meeting chairperson or organizer using the RMX Web Client to start your own meeting, you need to communicate the default conference ID (or the one you created) to the other conference participants so they can dial in.

You can use the **New Conference - General** dialog box to modify the conference parameters. If no defined participants are to be added to the conference, or you do not want to add additional information, click **OK**.

For more details, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Starting an AVC CP Conference from the Conferences Pane.

Starting a Reservation

To start a conference from the Reservation Calendar:

- 1 In the MCUs pane, select the MCU to run the conference.
- 2 In the RMX Management pane, click Reservation Calendar ().

Name of selected MCU

7 7 7 % - Product I Mo **172.22.186.45** 172.22.186.45 A Major RMX 40 🔽 2.22.190.40 172.22.190.40 06 172,22,190,40 A Empl 14 16 ° 18 19 Connecti A Users - Signaling Monto I Hardware Monit

The **Reservation Calendar** is displayed.

3 Click New Reservation ().

For more information, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Scheduling an AVC-based Reservation.

Starting an Ongoing Conference or Reservation From a Template

An ongoing conference or a Reservation can be started from any Conference Template saved in the *Conference Templates* list of the selected MCU.

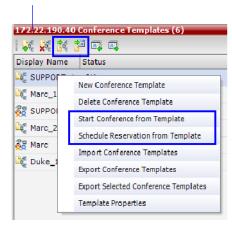
To start an ongoing conference or a reservation from a Template:

- 1 In the **MCUs** pane, select the MCU to run the conference.
- 2 In the Conference Templates list, select the Template you want to start as an ongoing conference.
- 3 Click Start Conference from Template () to start a conference or Schedule Reservation from Template () to schedule a reservation.

or

Right-click and select **Start Conference from Template** to start an ongoing conference or **Schedule Reservation from Template** to schedule a reservation.

Name of selected MCU



The conference is started.

For detailed description of Conference Templates, see Conference Templates.

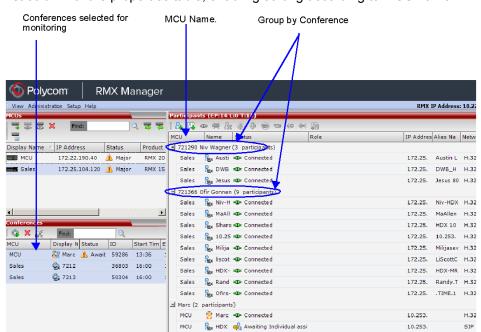
Monitoring Conferences

When MCUs are connected to the RMX Manager they are automatically monitored, that is, any ongoing conference that is started on that MCU is automatically added to the Conferences pane and its participants are monitored.

To list participants from several conferences (running on the same or different MCUs):

• In the **Conferences** pane, using Windows multiple selection methods, select the conferences whose participants you want to list.

The participants are displayed in the **Participants** list pane.



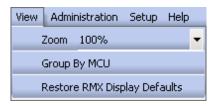
By default, the participants are grouped by conferences, and the name of the MCU is displayed in the first column of the properties table, enabling sorting according to MCU name.

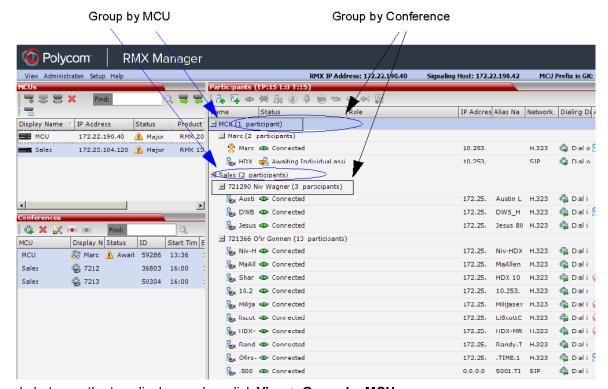
Grouping the Participants by MCU

The Participants can be grouped by MCU and then by conferences.

To change the display mode for the Participants pane:

On the Collaboration Server menu, click View > Group by MCU.





The Participants pane display changes accordingly.

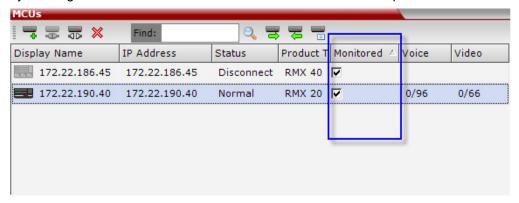
To toggle between the two display modes, click View > Group by MCU.

Start Monitoring/Stop Monitoring

By default, all conferences running on connected Collaboration Servers are monitored.

You can stop the automatic monitoring of conferences on a specific MCU in one of the following methods:

By clearing the check box in the Monitored column in the MCUs pane.

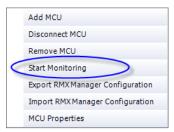


Right-clicking the MCU icon and selecting Stop Monitoring.



The check box is cleared in the Monitored column.

To start monitoring again, click the check box in the **Monitored** column in the **MCUs** pane, or right-clicking the MCU icon and selecting **Start Monitoring**.



Modifying the MCU Properties

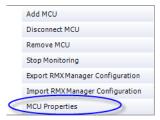
You can view the currently defined MCU settings, and modify them when required, for example, change the MCU name, IP address or Secured mode.

Use this procedure to add the **Username** and **Password** to the properties of the MCU that was automatically added to the MCU list when installing the RMX Manager. This enables automatic login when connecting the MCU to the RMX Manager.

You can modify the MCU properties when the MCU is connected or disconnected.

To view and/or modify the MCU Properties:

- **1** Use one of the following methods:
 - a Select the MCU to disconnect and click MCU Properties ...
 - **b** Right-click the **MCU** icon and then click **MCU Properties**.



The MCU Properties dialog box opens.

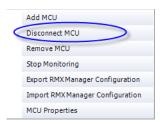
- **2** Define/modify the required parameters. For details, see MCU Properties.
- 3 Click OK.

Disconnecting an MCU

An MCU can be disconnected from the RMX Manager, without removing it from the MCUs list.

To disconnect an MCU:

- 1 Use one of the following methods:
 - a Select the MCU to disconnect and click Disconnect MCU ...
 - **b** Right-click the MCU icon and then click **Disconnect MCU**.



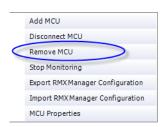
The MCU icon changes to disconnected and any ongoing conference running on that MCU will not be monitored in this RMX Manager; they are removed from the **Conferences** pane. This MCU can still be monitored and controlled by other users.

Removing an MCU from the MCUs Pane

An MCU can be removed from the RMX Manager. This function should be used if the MCU hardware was disconnected and removed from the network.

To Remove an MCU from the list:

- 1 Use one of the following methods:
 - a Select the MCU to disconnect and click **Delete**
 - b Right-click the MCU icon and then click Remove MCU.



A confirmation message is displayed.

2 Click **OK** to confirm or **Cancel** to abort the operation.

The MCU icon is removed from the MCUs pane.

Changing the RMX Manager Language

You can change the language of the RMX Manager menus and dialog boxes. Only one language can be selected at a time and the RMX Manager application must be restarted after changing the display language.

To select a language:

1 On the RMX Manager menu, click Setup > Customize Display Settings > Multilingual Settings.

The Multilingual Settings dialog box opens, displaying the current language selection.



- 2 Click the check box of the required language. Only one language can be selected.
- 3 Click OK.
- **4** Restart the RMX Manager application to implement the language change.

Import/Export RMX Manager Configuration

The RMX Manager configuration that includes the MCU list and the multilingual selection can be save to any workstation/PC on the network and imported to any Multi-RMX Manager installed in the network. This enables the creation of the MCUs list once and distributing it to all RMX Manager installations on the network.

In addition, when upgrading to a previous version, the MCU list is deleted, and can be imported after upgrade.

The exported file is save in XML format and can be edited in any text editor that can open XML files.

To Export the RMX Manager Configuration:

1 In the RMX Manager, click **Export RMX Manager Configuration** in the toolbar, or right-click anywhere in the **MCUs** pane and then click **Export RMX Manager Configuration**.



The **Export RMX Manager Configuration** dialog box opens.

2 Click Browse to select the location of the save file, or enter the required path in the Export Path box.

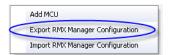


The selected file path is displayed in the **Export Path** box.

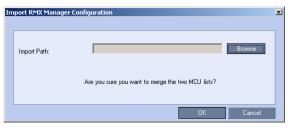
3 Click OK to export the RMX Manager configuration.

To Import the RMX Manager Configuration:

1 In the RMX Manager, click **Import RMX Manager Configuration** in the toolbar, or right-click anywhere in the **MCUs** pane and then click **Import RMX Manager Configuration**.

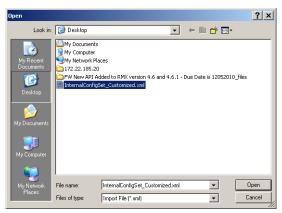


The **Import RMX Manager Configuration** dialog box opens.



2 Click the **Browse** button to select the saved file, or enter the required path in the **Export Path** box.

The **Open** dialog box is displayed.



- 3 Select the XML file previously saved, and click the Open button. The selected file path is displayed in the Import Path box.
- 4 Click **OK** to import the file.

Installing RMX Manager in Secure Communication Mode

The RMX Manager cannot be downloaded from an MCU operating in Secure Communication Mode, without a valid TLS certificate.

The following procedure describes how to obtain a TLS certificate and download the RMX Manager from the MCU operating in Secure Communication Mode.



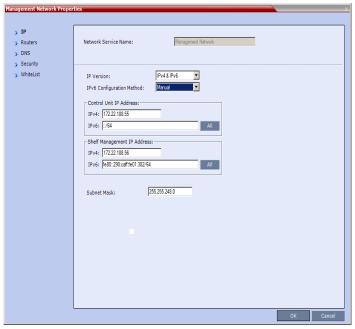
FIPS is always enabled in Ultra Secure Mode, and when **ClickOnce** is used to install RMX Manager, the workstation must have one of the following installed:

- .NET Framework 3.5 or a later version of the .NET Framework.
- .NET Framework 2.0 plus Service Pack 1 or later.

To install the RMX Manager:

- 1 Set the Collaboration Server to Non Secure Communication Mode
 - a In the RMX Management pane, click IP Network Services.
 - b In the IP Network Services list pane, double click the Management Network entry.





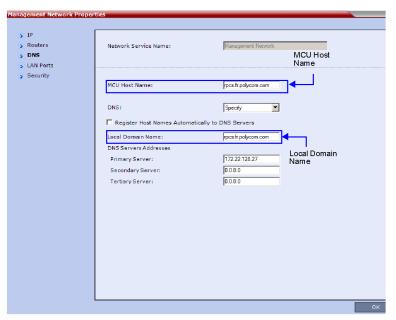
c Click on the Security tab.

The **Security** dialog box is displayed.



- d Clear the Secured Communication check box.
- 2 Click the DNS tab.

The **DNS** dialog box is displayed.

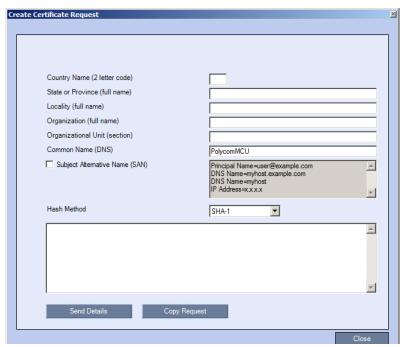


3 Enter the Local Domain Name.



The **Local Domain Name** must be the same as the **MCU Host Name**. If the content of these two fields are not identical an active alarm is created.

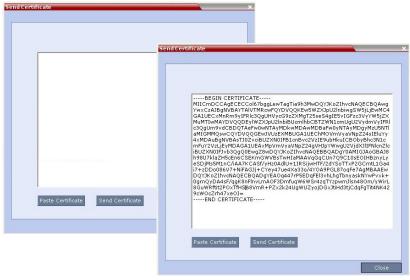
4 Create a Certificate Request.



For more information, see Purchasing and Installing a Certificate.

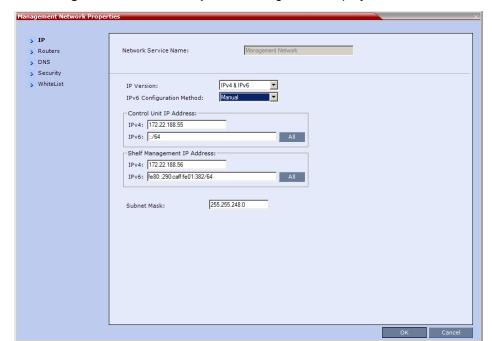
Certificates can also be created and issued using an *Internal Certificate Authority*. For more information see Using an Internal Certificate Authority.

5 Install the certificate.



For more information, see Purchasing and Installing a Certificate.

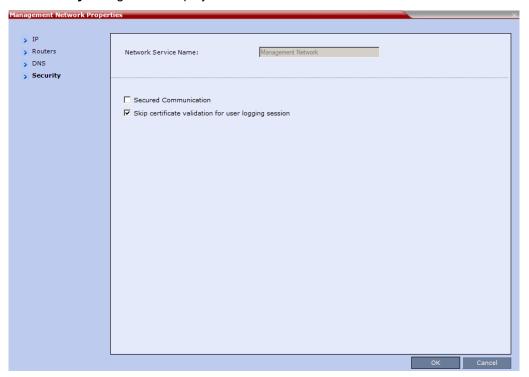
- 6 Set the Collaboration Server to Secure Communication Mode
 - a In the RMX Management pane, click IP Network Services.
 - b In the IP Network Services list pane, double click the Management Network entry.



The Management Network Properties dialog box is displayed.

c Click the Security tab.

The **Security** dialog box is displayed.



d Select the Secured Communication check box.

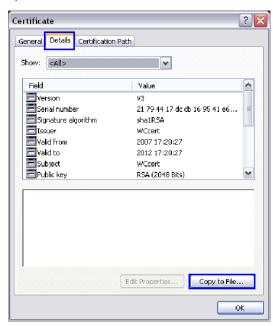
- e Click OK.
- **7** Reset the Collaboration Server:
 - a In the RMX Management pane, click Hardware Monitor.
 The Hardware Monitor pane is displayed.
 - b Click Reset (22).
- 8 Install the RMX Manager. For more information see Installing the RMX Manager Application.

Using an Internal Certificate Authority

If your TLS certificate was created and issued by an Internal Certificate Authority, it may not be seen as having been issued by a trusted Certificate Authority. The RMX Manager is not downloaded successfully and a warning is received stating that the certificate was not issued by a trusted Certificate Authority.

To add the Internal Certificate Authority as a trusted Certificate Authority:

- 1 Navigate to the folder where the certificate (.cer) file is saved.
- 2 Open the certificate file.



3 Click the **Details** tab.

4 Click the Copy to File button.

The Certificate Export Wizard is displayed.



5 Click Next.

The Export File Format dialog box is displayed.



- 6 Select Base-64 encoded X.509 (.CER).
- 7 Click Next.

The File to Export dialog box is displayed.



- 8 In the File Name field, enter the file name for the exported certificate.
- 9 Click Next.

The final Certificate Export Wizard dialog box is displayed.



10 Click the Finish button.

The successful export message is displayed.



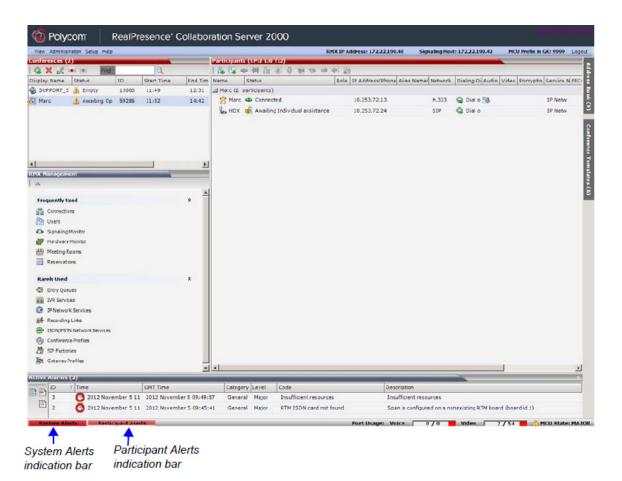
11 Click OK.

Administration and Utilities

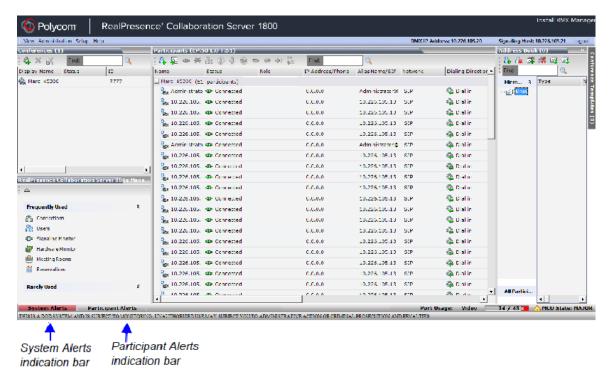
System and Participant Alerts

The MCU alerts users to any faults or errors the MCU encountered during operation. Two indication bars labeled System Alerts and Participant Alerts signal users of system errors by blinking red in the event of an alert.

Collaboration Server 1500/2000/4000 Status Bar



Collaboration Server 1800 Status Bar



The System Alerts indication bar blinks red prompting the user to view the active alarms. Once viewed, the System Alerts indication bar becomes statically red until the errors have been resolved in the MCU.

The Participants Alerts indication bar blinks red indicating participant connection difficulties in conferences. Once viewed, the Participant Alerts indication bar becomes statically red until the errors have been resolved in the MCU.

System Alerts

System Alerts are activated when the system encounters errors such as a general or card error. The system errors are recorded by the Collaboration Server and can be generated into a report that can be saved in *.txt format.

To view the System Alerts list:

1 Click the red blinking System Alerts indication bar.

The Active Alarms pane opens. This screen indicates what events have not been resolved.



The following columns appear in the **Active Alarms** pane:

Active Alarms Pane Columns

Field	Description					
ID	An identifying number assigned to the system alert.					
Time	Lists the local date and time that the error occurred. This column also includes the icon indicating the error level (as listed in the level column).					
GMT Time	Lists the date and time according to Greenwich Mean Time (GMT) that the error occurred.					
Category	Lists the type of error. The following categories may be listed: • File indicates a problem in one of the files stored on the MCU's hard disk. • Card indicates problems with a card. • Exception indicates software errors. • General indicates a general error. • Assert indicates internal software errors that are reported by the software program.					
Category (cont.)	 Startup indicates errors that occurred during system startup. Unit indicates problems with a unit. MPL indicates an error related to a Shelf Management component (MPL component) other than an MPM, RTM or switch board (Collaboration Server 1500/2000/4000 only). 					
Level	Indicates the severity of the problem, or the type of event. There are three fault level indicators: - Major Error - System Message - Startup Event					
Code	Indicates the problem, as indicated by the error category.					
Process Name	Lists the type of functional process involved.					
Description	When applicable, displays a more detailed explanation of the cause of the problem.					

For more information about the Active Alarms, see Appendix B - Active Alarms .

2 Click one of the following two buttons to view its report in the System Alerts pane:

System Alerts Buttons



Active Alarms (default) – this is the default reports list that is displayed when clicking the System Alerts indication bar. It displays the current system errors and is a quick indicator of the MCU status.



Faults Full List - A list of all system faults.

Note: Viewed when logged in as a special support user.



Faults List – a list of faults that occurred previously (whether they were solved or not) for support or debugging purposes.

- 3 To save the Active Alarms, Faults Full List or Faults report:
 - > to a text file, click the Save to Text button
 - > to an XML file, click the Save to XML in button



The Save to XML button is only available when logged in as a special support user.

The Save dialog window opens.

- 4 Select a destination folder and enter the file name.
- 5 Click Save.

Participant Alerts

Participant Alerts enables users, participants and conferences to be prompted and currently connected. This includes all participants that are disconnected, idle, on standby or waiting for dial-in. Alerts are intended for users or administrators to quickly see all participants that need their attention.

To view the Participants Alerts list:

1 Click the red blinking Participants Alerts indication bar.

The Participant Alerts pane opens.





The Participant Alerts pane displays similar properties to that of the Participant List pane. For more information, see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Participant Level Monitoring .

To resolve participant issues that created the Participant Alerts, the administrator can either Connect ♠, Disconnect ♠ or Delete ♠ a participant.

RMX Time

To ensure accurate conference scheduling, the MCU has an internal clock that can function in standalone mode, or in synchronization with up to three *Network Time Protocol (NTP)* servers.

NTP Servers can be used if:

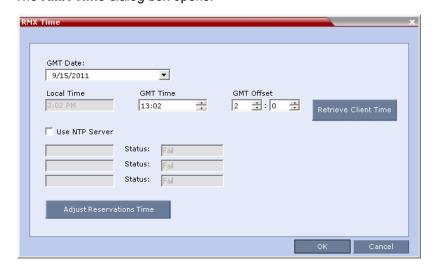
- NTP servers use Version 4 as it is the only supported protocol.
- If applicable, daylight saving adjustments must be implemented by the administrator whether the MCU is in standalone mode or synchronized with NTP Servers.

Altering the clock

The MCU's date and time can be set manually or enabled to synchronize with external NTP servers.

To Alter the MCU Time:

1 On the Collaboration Server menu, click Setup > RMX Time. The RMX Time dialog box opens.



2 View or modify the following fields:

RMX Time - Fields Properties

Field	Description
GMT Date	The date at Greenwich, UK.
Local Time	The MCU's local time settings, are calculated from the <i>GMT Time</i> and the <i>GMT Offset</i> .
GMT Time	The MCU's current <i>GMT Time</i> settings. Select the Up or Down arrows to alter the GMT Time on the MCU.

RMX Time – Fields Properties

Field	Description
GMT Offset	The time zone difference between Greenwich and the MCU's physical location in hours and minutes.
	Select the Up or Down arrows to alter the GMT Offset time on the MCU. To enter a negative offset either type a minus in the hour box or use the down arrow and decrease the offset below zero.
Retrieve Client Time	Click this button to automatically update the MCU's GMT Date, Time and Offset to match that of the workstation.
Use NTP Server	Select this check box to synchronize the time with up to three NTP servers. When selected, the manual GMT Date and GMT Time setting options are disabled. The GMT Offset fields are still active.
	To implement this mode an external connection to an NTP server must be enabled.
	Enter the IP addresses of the required NTP servers in order of precedence.
	The Status field indicates whether registration with the NTP Server failed or succeeded.
	Note : The Collaboration Server will not use a time source such as a Windows-based, W32Time service (SNTP) time service. Only full-featured (below Stratum 16) NTP Servers are considered sufficiently reliable for high-accuracy timing environments.
Adjust Reservations Time	Use this button to adjust the start time of all the reservations in one operation. For more information see Adjusting the Start Times of all Reservations.
(Button)	Not supported in the RealPresence Collaboration Server.



After resetting the MCU a delay may occur when synchronizing with the external NTP server.

Resource Management

This section describes how the MCU resources are managed by the MCU and how they are used by the MCU to connect participant to conferences.

This section describes:

Resource Capacity

AVC Conferencing - Voice

Video/Voice Port Configuration - MPMx

Displaying the Resource Report

MCU Resource Management by RealPresence Resource Manager (XMA), Polycom CMA and Polycom RealPresence DMA System

Resource Capacity

The MCU resources are determined by the MCU type, Card Configuration Mode and the system license you have purchased. The total number of licensed resources is shown in the System Information.

The Collaboration Server (RMX) 1500 supports one Card Configuration Mode: MPMx. The Collaboration Server (RMX) 1500 contains only one card and can have to 4 ISDN/PSTN E1/T1 connections.



Three assembly variations, MPMx-S, MPMx-D and MPMx-Q, differing in resource capacity, are available for the RealPresence Collaboration Server (RMX) 1500. For capacity details, see

The Collaboration Server (RMX) 2000 / 4000 can support two Card Configuration Modes: MPMx or MPMRx. The Collaboration Server (RMX) 2000 can include up to two media cards and one RTM-ISDN card with up to 7 E1 or 9 T1 connections.

The Collaboration Server (RMX) 4000 can include up to four media cards and one RTM-ISDN card with up to 7 E1 or 9 T1 connections.

The Collaboration Server (RMX) 1800 supports one media card type which is similar to the MPMRx card and therefore it is considered to support one Card Configuration Mode: MPMRx. It does not have ISDN/PSTN Connections.

MCU Capacities in CP Only Conferencing and SVC Only Conferencing

The following table summarizes the resource capacities of fully configured (with all media cards at their full capacity) and fully licenced Collaboration Servers with the various card types per resolution in AVC CP only Conferencing mode or in SVC only conferences (and not in mixed CP and SVC conferences).

Resource Capacities for Full Capacity Collaboration Server per Resolution in AVC CP Only or SVC Only

	Maximum Possible Resources per Collaboration Server Model								
Resource Type	1500	18	00*	2000**		4000**			
	MPMx	1 card	3 cards	MPMx	MPMRx-D	MPMx	MPMRx-D		
Voice (IP)	360	50	150	720	260	1440	520		
Voice (PSTN)	120	N/A	N/A	400	260	400	400		
CIF H.263	60	25	75	120	130	240	260		
CIF H.264	90	50	150	180	260	360	520		
CIF 60 H.264	60	12	37	120	65	240	130		
SD30 H.264	60	50	150	120	260	240	520		
4CIF H.263	30	25	75	60	130	120	260		
4CIF 60 / SD 60	30	12	37	60	65	120	130		
HD720p30	30	25	75	60	130	120	260		
HD1080p30 / HD720p60 Symmetric	15	12	37	30	65	60	130		
HD1080p60 Asymmetric	7	N/A	N/A	30	NA	60	NA		
HD1080p60 Symmetric	50	6	18	50	32	100	65		
SVC	90	75	225	180	390	360	780		

^{*} Collaboration Server 1800: For a maximum license of 75 ports.

Resource Usage in AVC CP Conferencing

Video resources usage varies according to the video resolution used by the endpoints. The higher the video resolution (quality), the greater the amount of video resources consumed by the MCU. The following table shows the number of video resources used for each resolution.

The port consumption ratios of different calls against that of a HD720p30 call are as shown in this table.

Port Consumption Ratios of Different Calls

Card Type/ Conferencing Mode	HD1080p60	HD1080p30	HD720p30	AVC SD	AVC CIF	Audio	svc
MPMRx CP only or SVC only	4	2	1	0.5	0.5	0.5	0.3333

^{**} Collaboration Server 2000/4000: For a maximum license of 65 ports.

MPMx CP only or SVC only	N/A	2	1	0.5	0.3333	0.0833	0.3333

Resource Usage in SVC Conferencing

During a SVC conference, each SVC-endpoint uses a video port that is equivalent to a third of HD720p30 port. When sharing content an additional video resource is used.

MCU Capacities in Mixed CP and SVC Conferencing

In a mixed CP and SVC conference, video resources are used according to the amount of both AVC and SVC participants in the conference.

Resource Capacities for Full Capacity Collaboration Server per Resolution in Mixed CP and SVC Conferencing

	Maximum Possible Resources per Collaboration Server Model							
Resource Type	1500	1800*		20	2000**		4000**	
	MPMx	1 card	3 cards	MPMx	MPMRx-D	MPMx	MPMRx-D	
Voice (IP)	360	26	75	720	150	1440	300	
Voice (PSTN)	120	N/A	N/A	400	150	300	300	
CIF H.264		26	75		150		300	
SD30 H.264/4CIF	30	26	75	60	150	120	300	
HD720p30	20	14	42	40	84	80	168	
HD1080p30	10	8	25	20	42	40	84	
HD1080p60	5	NA	NA	10	NA	20	NA	
SVC	90	52	150	180	300	360	600	

^{*} Collaboration Server 1800: For a maximum license of 75 ports for 3 cards and 25 ports for 1 card configurations.

Resource Usage in Mixed CP and SVC Conferencing

Port Consumption Ratios of Different Calls

Card Type/ Conferencing	HD1080p60	HD1080p30	HD720p30	AVC SD	AVC CIF	Audio	svc
Mode							

^{**} Collaboration Server 2000/4000: For a maximum license of 65 ports.

MPMRx mixed CP and SVC	N/A	3	1.5	0.75	0.75	0.75	0.3333
MPMx mixed CP and SVC	N/A	3	1.5	0.75	0.75		

AVC Conferencing - Video Switching Resource Capacity (Collaboration Server 1500/2000/4000 Only)

During a Video Switching conference, each endpoint uses one video (CIF) port.

The following table summarizes the resource capacities of fully configured MCUs with the various card types per line rate in VSW Conferencing mode.

Resource Capacity Allocation per Line Rate in VSW Conferencing Mode

	Maximum Possible Resources (CIF Video Resources)							
Resource Type	RMX 1500	RMX	2000	RMX 4000				
	MPMx	MPMx	MPMRx	MPMx	MPMRx			
Voice (IP)	360	720	260	1440	520			
Voice (PSTN)	120	400	260	400	400			
VSW 2Mb	80	160	130	320	260			
VSW 4Mb	40	80	130	160	260			
VSW 6Mb	20	40	120	80	240			
ISDN		7 E1 or	9 T1 (per RTM ISC	N card)				



MCUs with 500MB of memory can support a maximum of 400 simultaneous participant calls, regardless of how system resources are allocated.

MCUs with 1000MB of memory are not subject to this limitation.

MCU memory size is listed in the **Administration > System Information** properties box. For more information see System Information .

Resource Usage in AVC CP Conferencing

Video resources usage varies according to the video resolution used by the endpoints. The higher the video resolution (quality), the greater the amount of video resources consumed by the MCU. Table 5-5 shows the number of video resources used for each resolution.

HD720p30 Equivalent Video Resource Usage vs. Resolution

Decelution/free	HD Video Resources	S Used per Collabor	ration Server Model
Resolution/fps	1500 / 2000 / 4000 MPMx	1800	2000 / 4000 MPMRx
H.261 CIF 30fps	2/3		
H.263 CIF 30fps	1/3	1	1/2
H.263 4CIF 30fps	1/3	1	1/2
H.264 CIF 30fps	1/3	1/2	1/2
H.264 CIF 60fps	1/3	2	2/3
H.264 4CIF 30fps	1/3	1/2	1/2
H.264 4CIF 60fps	1/3	2	2/3
H.264 720p 30fps	1/3	1	1
H.264 720p 60fps	2/3	2	2
H.264 1080p 30fps	2/3	2	2
H.264 1080p 60fps	4/3	4	4
SVC	1/3	1/3	1/3

AVC Conferencing - Voice

In Collaboration Server 1500/2000/4000 in **MPMx** Card Configuration Mode, one Audio Only resource is used to connect a single voice participant when CIF resources have been converted to Audio Only. However, if no CIF resources were converted, Audio Only endpoints use one CIF video resource per connection.

When video ports are fully used, the system cannot use free audio ports for video. When audio port resources are fully used, video ports can be used, using one video port to connect one voice participant.

In Collaboration Server 1500/1800/2000/4000 in **MPMRx** Card Configuration Mode, a voice port equals a CIF video port and there is no differentiation between voice and video ports.

Resource Capacity Modes

The installed media card type (MPMx or MPMRx) determines the Card Configuration Mode, which in turn determines the resource allocation method that can be selected for the MCU. The resource allocation method determines how the system resources are allocated to the connecting endpoints and it is defined in the Video/Voice Port Configuration. Two allocation methods are available:

Flexible Resource Capacity™ – This is the default allocation mode that is used in all versions and
can be used in all Card Configuration Modes and applies to all Conferencing Modes (SVC and AVC
conferencing). The resources are only set to audio and video as a pool and the system allocates the
resources according to the connecting endpoints. This mode offers flexibility in resource allocation
and is available in MPMx and MPMRx Card Configuration Modes.

In Flexible Resource Capacity mode, in MPMx and MPMRx Card Configuration Modes, the maximum number of resources is based on the system license, regardless of the hardware configuration of the MCU. These resources are allocated as CIF resources by default.

Example: If the MCU is licensed for 80 video resources, but only one Media card is currently installed in the MCU, the system lets you allocate 80 ports although only 40 video resources are available for participant connection. (However, an active alarm will be added to the *Active Alarms* list indicating a resource deficiency).



From Version 8.1, only the MPMx Media Card and Card Configuration Mode are supported.

Video/Voice Port Configuration - MPMRx

Although the Video/Voice Configuration dialog box is displayed for Collaboration Servers 2000/4000 with MPMRx media cards installed, Video/Voice Configuration is not supported.

These MCUs and the **Collaboration Server 1800** will allocate the same amount of system resources to voice (audio) participants, as those allocated to CIF video participants. For more information see Resource Reports .

Video/Voice Port Configuration - MPMx

The *Video/Voice Port Configuration* dialog box enables you to configure the resources per resource type using Flexible Resource Capacity Mode if the MCU has MPMx media cards installed.



From Version 8.1, Fixed Resource Capacity mode is disabled and cannot be selected in the Video/Voice Port Configuration.

If Fixed Resource Capacity mode was active at the time of an upgrade, Flexible Resource Capacity mode will automatically be enabled, the settings from the last time Flexible Resource Capacity mode active on the Collaboration Server are implemented when the upgrade is complete.

Flexible Resource Capacity Mode

Flexible Resource Capacity is the default mode for MPMx media cards.

All resources are initially allocated as HD720p30 video ports. The administrator can allocate some or all of these resources as *Voice* resources and let the system allocate the remaining *Video* resources automatically as participants connect to conferences. The number of resources automatically allocated by the system resources per endpoint is according to the participant's endpoint type, capabilities and line rate.



If the system runs out of voice ports, voice endpoints cannot connect to available video ports. Conversely, video endpoints cannot connect to available voice ports.

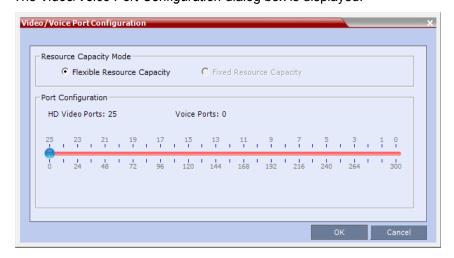
Configuring the Video/Voice Resources



- Resource re-configuration should only be performed when no conferences are running on the MCU.
- Updating the configuration sequentially requires a 10 seconds wait between updates, to let the system complete the update process.

To allocate Voice resources:

1 In the RMX menu, click Setup > Video/Voice Port Configuration.
The Video/Voice Port Configuration dialog box is displayed.



A slider is displayed, calibrated according to the number of HD720p30 video licenses purchased for the MCU.

- 2 Move the slider (to the right) to increase the number of *Voice* ports allocated.
 As the slider moves, HD72p30 video ports are converted to voice ports, with each HD72p30 video port converting to 12 voice ports.
- 3 Click OK.



On the RMX1500 MPMx-Q assembly, the use of HD with Continuous Presence requires an additional license. In the Resource Report and Resolution Configuration panes, HD settings are displayed but are not enabled and if HD is selected the system will enable SD by default.

Forcing Video Resource Allocation to CIF Resolution

You can set the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution determined by the Conference Profile parameters. This forcing saves resources and enables more endpoints to connect to conferences.

The forcing is done by modifying the system configuration and it applies to all conferences running on the MCU.

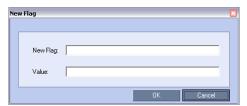
You can specify the endpoint types for which resource allocation can be forced to CIF resource, enabling other types of endpoints to use higher resolutions in the same conference. For example, you can force the system to allocate one CIF video resource to CMAD and VSX endpoints while HDX endpoints can connect using SD or HD video resources.

Once the endpoint connects to the conference, its type is identified by the Collaboration Server and, if applicable, the Collaboration Server will connect it using one CIF resource, even if a higher resolution can be used.

To force CIF resource:

- 1 On the Collaboration Server menu, click Setup > System Configuration. The System Flags dialog box opens.
- 2 In the MCMS_PARAMETERS tab, click the New Flag button.

The New Flag dialog box is displayed.



- 3 In the New Flag field enter the flag name: FORCE CIF PORT ALLOCATION
- **4** In the *Value* field enter the product type to which the CIF resource should be allocated. Possible values are:
 - CMA Desktop for CMA desktop client
 - > VSX nnnn where nnnn represents the model number for example, VSX 8000.

You can define several endpoint types, listing them one after the other separated by semicolon (;). For example, CMA Desktop; VSX 8000.

5 Click OK.

The new flag is added to the flags list.

Reset the MCU for changes to take effect. For more details, see the .

To cancel the forcing of CIF resource:

- 1 On the Collaboration Server menu, click **Setup > System Configuration**.
 - The System Flags dialog box opens.
- 2 In the MCMS_PARAMETERS tab, double-click or select the flag FORCE_CIF_PORT_ALLOCATION and click the Edit Flag button.
- 3 In the New Value field, clear the value entries.
- 4 Click OK.

Reset the MCU for changes to take effect. For more details, see the .

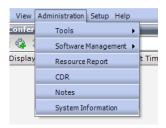
Resource Reports

When viewing the Collaboration Server resource report, the resource allocations are described in AVC HD720p30 units.

The Resource Report also includes a graphic representation of the resource usage. One resource report is available for all resource usage including SVC-based endpoints.

Displaying the Resource Report

1 In the main toolbar, click Administration > Resource Report.



For each resource type, the Resource Report includes the following columns:

Resource Report Fields Parameters

Column	Description
Туре	The type of audio/video resources available. This applies to both AVC and SVC-based endpoints (and resources).
Occupied	The number of MCU resources that are used by connected AVC and SVC-based participants or reserved for defined participants.
Free	The number of MCU resources available for connecting AVC and SVC-based endpoints.
Total	The <i>Total</i> column displays the total number of resources of that type as configured in the system (<i>Occupied</i> and <i>Free</i>). This number reflects the current audio/video port configuration (for AVC and SVC-based conferencing). Any changes to the resource allocation will affect the resource usage displayed in the Resource Report.

Resource Report for Collaboration Servers 1500 and 2000/4000 with MPMx media cards

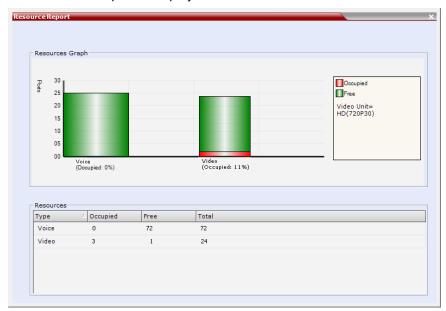
The Resource Report details the current availability and usage of the system resources for both AVC and SVC-based endpoint, displaying the number of free and occupied audio and video resources. A Resources Graph is displayed in addition to the Resources table.

Example: A Collaboration Server with MPMx media cards installed has:

- 30 licensed HD720p30 resources.
- 6 of its 30 HD720p30 resources allocated as Audio = 72 Audio resources (6x12).
- All 72 Audio resources free (green).

- The remaining 24 HD720p30 resources allocated as Video resources.
- 3 of the 24 HD720p30 resources are occupied (red) while the remaining 21 are free.

The Resource Report is displayed as follows:



Resource usage is displayed for *Voice* and Video resources, where the number of video resources is represented in the equivalent of *HD720p30* resources. The number represents a pool of both AVC and SVC resources. They are displayed as percentages of the total resource type.

The actual number of occupied or free resources can also be displayed by moving the cursor over the columns of the bar graph. Moving the cursor over the *Video* bar displays the following:



Port Gauges

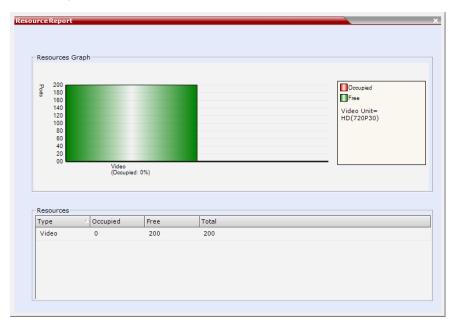
The *Port Gauges* in the *Status Bar* show the numbers as they appear in the resource report. In the following example, 0 of the 40 *Audio (Voice)* resources are shown as occupied and 8 of the 72 *Video* resources are shown as occupied.



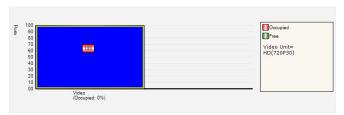
Resource Reports for Collaboration Server 1800 and 2000/4000 with MPMRx media cards

Collaboration Servers with MPMRx media cards installed do not differentiate between Video and Voice (Audio) resources. These MCUs allocate the same amount of system resources to Voice (Audio) participants, as those allocated to CIF Video participants.

Example: A Collaboration Server with MPMRx media cards installed has 200 licensed *HD720p30* resources, all of which are free.



The actual number of occupied or free resources can also be displayed by moving the cursor over the columns of the bar graph. Moving the cursor over the *Video* bar displays the following view:



Port Gauge

The *Port Gauge* in the *Status Bar* show the numbers as they appear in the resource report. In the following example, 20 of the 400 system resources are shown as occupied.

Port Usage: 20 / 400

Resource Capacities in AVC CP, SVC and Mixed Mode Conferences in MPMx Card Configuration Mode

When viewing the Collaboration Server resource report for mixed CP and SVC conferences, the resource allocations are described in AVC HD720p30 units. A port ratio of 1 AVC HD port will equal 2 AVC SD ports, which equals 3 SVC ports (in a non-mixed conference). When the Collaboration Server is reporting the available capacity, it will appropriately round up the remaining capacity to the nearest whole value of available ports. For example, one SVC endpoint in a conference is equal to 1/3 of the resource value. The resource report displays this as one full resource used. Two SVC endpoints is equal to 2/3 of the resource value. Therefore, the resource report displays this as one full resource used, and so forth. The following tables show the actual resource capacity utilization for both CP only and mixed CP and SVC conferences in AVC HD720p30 units for each port type for a single MPMx media board at full capacity.

Resource Capacity Allocation Per Port Type

Port Type	Non-Mixed Conferences	Mixed CP and SVC Conferences
AVC HD	1	1.5 *
AVC SD	0.5	0.75 *
AVC CIF	0.333	0.75 *
SVC	0.333	0.333

^{*} Resources are consumed at this rate only after the conference contains a mix of endpoints.

Resource Capacity Utilization Per Port Type per MPMx Card

Port Type	Maximum Ports in Non-mixed Conferences	Maximum Ports in Mixed CP and SVC Conferences
Maximum number of licences		30
AVC HD	30	20
AVC SD	60	40
AVC CIF	90	40
SVC	90	90

Resource Capacities in AVC CP, SVC and Mixed Mode Conferences in MPMRx Card Configuration Mode

The Collaboration Server Model 1800, and Models 2000/4000 Resource Capacities are set out below.

Collaboration Server 1800 Resource Capacity

The RMX 1800 system allocates port resources in AVC HD 720 p30 units. The number of unit ports each types of calls requires differs for AVC-SVC mixed conferences and non-mixed conferences.

Listed are the resource capacities for different system configurations, licenses, and conferencing modes.

Resource Capacity in Non-Mixed Conferences

The port consumption ratios of different calls against that of a HD 720 p30 call are as shown in this table.

Port consumption ratios of different calls

HD720p 30	HD1080p 60	HD1080p 30	SD	CIF	Audio	svc
1	4	2	1/2	1/2	1/2	1/3

In other words, to make a 1080p60 call, you need four 720p 30 ports; to make a 1080p 30 call, two 720p 30 ports; and so forth.

When the required resource is not a whole number, it's rounded up to the nearest whole number. For example, to make an SVC call requiring 1/3 of an HD 720 p30 port. In fact, one port will be allocated.

Resource Capacity in Mixed Conferences

The the port consumption of different calls in mixed conferences are shown in the following table.

Port Consumption Ratios, in Mixed Conferences

HD720p30	HD1080p60	HD1080p30	AVC SD	AVC CIF	Audio	svc
1.5	NA	3	3/4	3/4	3/4	1/3

In other words, to make one 720 p30 call in a mixed conference, you need two license ports; to make one 1080 p30 call, three license ports; and so forth.

When the required resource is not a whole number, it's rounded up to the nearest whole number. For example, to make an SVC call requiring 1/3 of a license port. In fact, one port will be allocated.

For more information about resources licenses and capacities for the various Collaboration Server 1800 media card configurations, see the *Realpresence Collaboration Server (RMX)* 1800 Hardware Guide.

Collaboration Server 2000/4000 Resource Capacity

The Collaboration Server Models 2000/4000 Resource Capacities are set out below.

Resource Capacity in Non-Mixed Conferences

The port consumption ratios of different calls against that of a HD720p30 call are as shown in this table.

Port Consumption Ratios of Different Calls

HD720p30	HD1080p60	HD1080p30	AVC SD	AVC CIF	Audio	svc
1	4	2	1/2	1/2	1/2	1/3

In other words, to make one1080p60 call, you need 4x 720p 30 ports; to make one 1080p 30 call, 2x 720p 30 ports; and so forth.

When the required resource is not a whole number, it's rounded up to the nearest whole number. For example, to make an SVC call requiring 1/3 of an HD720p30 port. However in the *Port Gauge*, one port appears allocated.

Resource Capacity in Mixed Conferences

The following table shows the port consumption ratios of different calls against that of an HD720p30 call.

Port Consumption Ratios, in Mixed Conferences

HD720p30	HD1080p60	HD1080p30	AVC SD	AVC CIF	Audio	svc
1.5	NA	3	3/4	3/4	3/4	1/3

In other words, to make one 1080p30 call, you need 3x 720p30 ports; to make one 720p30 call, 1.5x 720p30 ports; and so forth.

When the required resource is not a whole number, it's rounded up to the nearest whole number. For example, to make an SVC call requiring 1/3 of an HD720p30 port. However in the *Port Gauge*, one port appears allocated.

For more information about resources licenses and capacities for the various Collaboration Server 2000/4000 media card configurations, see the *Realpresence Collaboration Server (RMX) 2000 Hardware Guide* and *Realpresence Collaboration Server (RMX) 4000 Hardware Guide*.

ISDN/PSTN

The RMX 1500 supports one ISDN card with 4 E1/T1 PRI lines.

On the *RMX 2000/4000* a maximum of two *RTM ISDN* cards are supported, each providing connection for up to either 7 *E1* or 9 *T1 PRI* lines.

On RMX 1500/2000/4000, E1 and T1 connections cannot be used simultaneously.

The following table lists the *ISDN* supported bit rates and their respective participant connection capacities per *RTM ISDN* card:

ISDN - E1/T1 Connection Capacity vs. Bit rate

Bit Rates (Kbps) (Bonded)	Number of Participants per RTM ISDN Card						
	E1	T1					
128	40	40	If the conference bit rate is 128Kbps, participants connecting at bit				
192	40	40	rates lower than 128Kbps are disconnected.				
256	40	40	If the conference bit rate is above 128Kbps but does not mate any of the bonded bit rates, participants are connected at the highest bonded bit rate that is less than the conference bit rate For example: If the conference bit rate is 1024Kbps, the participant is connected at 768Kbps.				
320	40	40					
384	34	34					
512	25	25	participant to connected at 7 cortope.				
768	17	17					
1152	11	11					
1472	9	9					
1536	8	8					
1920	7	6					

MCU Resource Management by RealPresence Resource Manager (XMA), Polycom CMA and Polycom RealPresence DMA System

When the RealPresence Resource Manager (XMA), Polycom CMA and Polycom RealPresence DMA system are part of the solution, following a request by the RealPresence Resource Manager (XMA), Polycom CMA or Polycom RealPresence DMA system, the *MCU* will send updates on resource usage to both *CMA* and *DMA*, with each application updating its own resource usage for the *MCU*. This provides better management of the *Collaboration Server* resources by the RealPresence Resource Manager (XMA), Polycom CMA and Polycom RealPresence DMA system.

Guidelines

- Resource usage updates from RMX to the CMA and DMA are supported only with RMXs with MPMx cards.
- Following requests sent by CMA and RealPresence DMA system, the Collaboration Server will send
 the number of occupied resources for a conference or total for the MCU.In Flexible Resource
 Capacity Mode, CMA/DMA receive information about how many Video (CIF) and Audio resources are
 occupied per conference or MCU according the request type sent by the CMA and DMA.
- Occupied resources are resources that are connected to ongoing conferences. Disconnected endpoints in an ongoing conference are not counted as occupied resources.

- An ongoing conference that does not include participants and the Send Content to Legacy Endpoints
 option is disabled does not occupy resources. If the Send Content to Legacy Endpoints option is
 enabled, the conference occupies one SD resource.
- The Collaboration Server is unaware of the resource usage split between the CMA and RealPresence DMA system.

Port Usage Threshold

The *Collaboration Server* can be set to alert the administrator to potential port capacity shortages. A capacity usage threshold can be set as a percentage of the total number of licensed ports in the system.

When the threshold is exceeded, a *System Alert* is generated.

The default port capacity usage threshold is 80%.

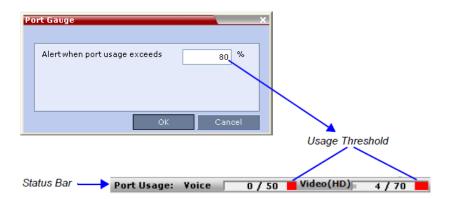
The administrator can monitor the MCU's port capacity usage via the *Port Gauges* in the *Status Bar* of the *Collaboration Server Web Client*.

Setting the Port Usage Threshold

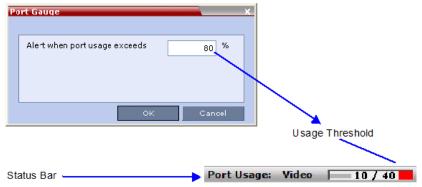
To Set the Port Usage Threshold:

1 In the Setup menu, click **Port Gauge** to open the Port Gauge dialog box.

Port Gauge Threshold Setting - RealPresence Collaboration Server (RMX) 1500/2000/4000 with MPMx Cards



Port Gauge Threshold Setting - RealPresence Collaboration Server 1800 and RealPresence Collaboration Server (RMX) 2000/4000 with MPMRx Cards



2 Enter the value for the percentage capacity usage threshold.

The value is applied to the Audio and video resources according to the Video/Voice Port Configuration.

The high Port Usage threshold represents a percentage of the total number of video or voice ports available. It is set to indicate when resource usage is approaching its maximum, resulting in no free resources to run additional conferences. When port usage reaches or exceeds the threshold, the red area of the gauge flashes. The default port usage threshold is 80%.

3 Click OK.

SIP Dial-in Busy Notification

When the system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the default), it enables the MCU to send a busy notification to a SIP audio endpoint or a SIP device when dialing in to the MCU whose audio resource usage exceeded the Port Usage threshold.

The Collaboration Server will send a SIP busy response to SIP audio endpoints when:

- The system flag SEND_SIP_BUSY_UPON_RESOURCE_THRESHOLD is set to YES (NO is the
 default)
- The port usage threshold for Audio resources is exceeded. The threshold is defined in the Setup > Port Gauge dialog box.



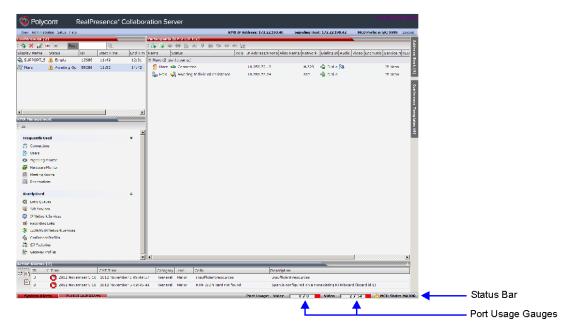
When the flag is set to YES, the system will allow SIP audio endpoints to connect to the MCU until the Port Usage threshold is reached. Once this threshold is exceeded, the SIP audio endpoints will not be able to connect, ensuring that the remaining system resources can be used by all other connections, including SIP video H.323 cascaded links and ISDN video. When the call is rejected by the MCU because of lack of resources, the appropriate indication will be sent by the MCU to the SIP audio endpoint.

For example, if the *Port Gauge* threshold is set to 80%, when 80% of the **Audio resources** are used, the system will not allow additional SIP audio endpoints to connect and will send a busy notification to the endpoint.

This does not affect the video resources usage.

Port Usage Gauges

The Port Usage Gauges are displayed in the *Status Bar* at the bottom of the Collaboration Server Web Client screen.



Port Usage Gauges

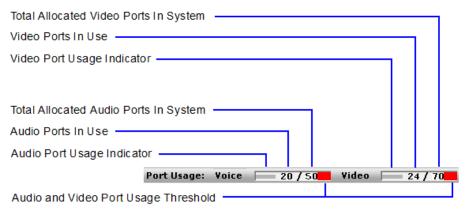
In the RealPresence Collaboration Server (RMX) 1500/2000/4000, the *Port Usage* gauges displays for the selected MCU:

- The total number of Video or Voice ports in the system according to the Video/Voice Port
 Configuration. The Audio gauge is displayed only if Audio ports were allocated by the administrator,
 otherwise only the Video port gauge is displayed.
- The number of Video and Voice ports in use.
- The High Port Usage threshold.

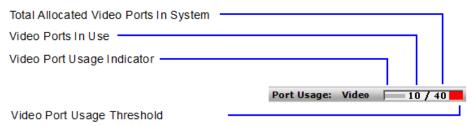
In the RealPresence Collaboration Server 1800 and the RealPresence Collaboration Server (RMX) 2000/4000 with an MPMRx card, the Port Usage Gauge displays for the selected MCU:

- The total number of Video ports in the system.
- The number of *Video*ports in use.
- The High Port Usage threshold.

Port Gauges - RealPresence Collaboration Server (RMX) 1500/2000/4000 with MPMx cards



Port Gauges - RealPresence Collaboration Server 1800 and RealPresence Collaboration Server (RMX) 2000/4000 with MPMRx cards



The basic unit used for reporting resource usage in the Port Gauges is HD720p30. Results are rounded to the nearest integer.

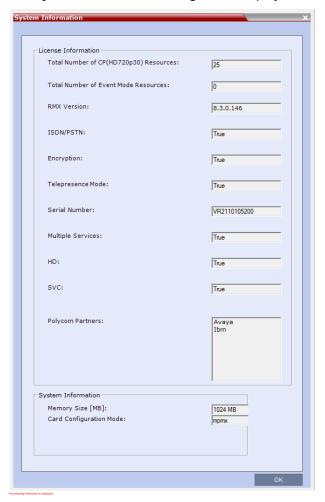
System Information

System Information includes License Information and general system information, such as system memory size and Media Card Configuration Mode.

To view the System Information properties box:

• On the Collaboration Server menu, click **Administration > System Information**.

The System Information dialog box is displayed.



System Information

Field	Description
Total Number of CP (HD720p30) Resources	Displays the number of HD720p30 video resources licensed for the system. Each HD720p30 resource represents 3 CIF video resources. Each SVC resource is equivalent to one CIF video resource.
Total Number of Event Mode Resources	Displays the number of video/voice resources licensed for a system in Event Mode Licensing. It also determines the conference type that is available on the system. 0 - indicates that this Licensing mode is disabled for this system.
RMX Version	Displays the System Software Version of the MCU.
ISDN/PSTN	Indicates whether RTM ISDN hardware has been detected in the system and if ISDN/PSTN is included in the MCU license. Range: True / False

System Information (Continued)

Field	Description	
Encryption	Indicates whether Encryption is included in the MCU license. Encryption is not available in all countries. Range: True / False	
Telepresence Mode	The field value indicates whether the system is licensed to work with RPX and TPX Telepresence room systems. Range: True / False	
Serial Number	Displays the Serial Number of the Collaboration Server unit.	
Multiple Services	Indicates if a Multiple Services license is installed.	
HD	Indicates if the MCU is licensed to connect endpoints at HD resolutions in Continuous Presence conferences.	
SVC	Indicates if the MCU is licensed to run SVC-based conferences.	
Polycom Partners	Indicates that the System Software contains features for the support of specific Polycom Partner environments.	
Memory Size [MB]	Indicates the MCU system memory size in Megabytes. Note: If Memory size is 512MB (Collaboration Server 1500/2000/4000 only), Version 7.1 and later are not supported. DO NOT upgrade the system to Version 7.1 and later.	
Card Configuration Mode	 Indicates the MCU configuration as derived from the installed media cards: MPMx: Only MPMx cards are supported. Any other media card in the system is disabled. MPMRx: Only MPMRx cards are supported. Any other media card in the system is disabled. Note: MPM and MPM+ Card Configuration Modes are not supported with this version. The RMX only switches between MPMx and MPMRx Card Configuration Modes if MPMx or MPMRx cards are removed or swapped while it is powered on. The Card Configuration Mode switch occurs during the next restart. Installing or swapping MPMx or MPMRx cards while the system is off will not cause a mode switch when the system is restarted; it will restart in the Card Configuration Mode that was active previous to powering down. 	

SNMP (Simple Network Management Protocol)

SNMP enables managing and monitoring of the MCU status by **external** managing systems, such as HP OpenView or through web applications.

The Collaboration Server's implementation of SNMPv3 is FIPS 140 compliant.

MIBs (Management Information Base)

MIBs are a collection of definitions, which define the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each of the definitions written in the MIB.

The SNMP systems poll the MCU according to the MIB definitions.

Traps

The MCU is able to send Traps to different managers. Traps are messages that are sent by the MCU to the SNMP Manager when an event such as MCU Reset occurs.

Guidelines

- Version 1, Version 2 and Version 3 traps are supported.
- When SNMPv3 is selected only SNMPv3 Queries and Traps receive responses.
- A mixture of Version 1, Version 2 and Version 3 traps is not permitted.
- In Ultra Secure Mode:
 - > Version 3 is the default for both SNMP Agent Version and SNMP Trap Version.
 - The default Authentication Protocol is SHA
 - > The default Privacy Protocol is AES.

MIB Files

The H.341 standard defines the MIBs that H.320 and H.323 MCUs must comply with. In addition, other MIBs should also be supported, such as MIB-II and the ENTITY MIB, which are common to all network entities.

The MIBs are contained in files in the SNMP MIBS sub-directory of the Collaboration Server root directory. The files should be loaded to the SNMP external system and compiled within that application. Only then can the SNMP external application perform the required monitoring tasks.



The MULTI-MEDIA MIB TC must be compiled before compiling the other MIBs.

Private MIBs

- RMX-MIB (RMX-MIB.MIB)
 - Contains the statuses of the Collaboration Server: Startup, Normal and Major.
 - > Contains all the Alarms of the Collaboration Server that are sent to the SNMP Manager.

Support for MIB-II Sections

The following table details the MIB-II sections that are supported:

Supported MIB-II Sections

Section	Object Identifier
system	mib-2 1
interfaces	mib-2 2
ip	mib-2 4

The Alarm-MIB

MIB used to send alarms. When a trap is sent, the Alarm-MIB is used to send it.

H.341-MIB (H.341 - H.323)

- Gives the address of the gatekeeper.
- Supports H.341-MIB of SNMP events of H.323.

Standard MIBs

This section describes the MIBs that are included with the Collaboration Server. These MIBs define the various parameters that can be monitored, and their acceptable values.

Standard MIBs

MIB Name	Description	
MULTI-MEDIA-MIB-TC (MULTIMTC.MIB)	Defines a set of textual conventions used within the set of Multi Media MIB modules.	
H.320ENTITY-MIB (H320-ENT.MIB)	This is a collection of common objects, which can be used in an H.320 terminal, an H.320 MCU and an H.320/H.323 gateway. These objects are arranged in three groups: Capability, Call Status, and H.221 Statistics.	
H.320MCU-MIB (H320-MCU.MIB)	Used to identify managed objects for an H.320 MCU. It consists of four groups: System, Conference, Terminal, and Controls. The <i>Conference</i> group consists of the active conferences. The <i>Terminal</i> group is used to describe terminals in active MCU conferences. The <i>Controls</i> group enables remote management of the MCU.	
H323MC-MIB (H323-MC.MIB)	Used to identify objects defined for an H.323 Multipoint Controller. It consists of six groups: System, Configuration, Conference, Statistics, Controls and Notifications. The <i>Conference</i> group is used to identify the active conferences in the MCU. The <i>Notifications</i> group allows an MCU, if enabled, to inform a remote management client of its operational status. Note: The Collaboration Server supports only one field in H.341-H323MC MIB. The Collaboration Server reports the Gatekeeper address using H.341-H323MC MIB – 323McConfigGatekeeperAddress (0.0.8.341.1.1.4.2.1.1.4) in response to a query from a manager.	

Standard MIBs (Continued)

MIB Name	Description
MP-MIB (H323-MP.MIB)	Used to identify objects defined for an H.323 Multipoint Processor, and consists of two groups: Configuration and Conference. The <i>Configuration</i> group is used to identify audio/video mix configuration counts. The <i>Conference</i> group describes the audio and video multi-processing operation.
MIB-II/RFC1213-MIB (RFC1213.MIB)	Holds basic network information and statistics about the following protocols: TCP, UDP, IP, ICMP and SNMP. In addition, it holds a table of interfaces that the Agent has. MIB-II also contains basic identification information for the system, such as, Product Name, Description, Location and Contact Person.
ENTITY-MIB (ENTITY.MIB)	Describes the unit physically: Number of slots, type of board in each slot, and number of ports in each slot.

Unified MIB

The Collaboration Server uses the Polycom Unified MIB, in addition to the RMX specific MIB. The Polycom Unified MIB is an MIB that is used by many Polycom products. The following table describes the information provided by the Collaboration Server in the Unified MIB.

Unified MIB SNMP Fields

Name	Туре	Description
Debug	Boolean	Indicates whether the unit is in a debugging state.
IncomingCallsReqrGK	Boolean	Indicates whether a gatekeeper is required to receive incoming H.323 calls.
OutgoingCallsReqrGK	Boolean	Indicates whether a gatekeeper is required to make outgoing H.323 calls.
HDBitrateThrshld	Integer	The minimum bit rate required by endpoints in order to connect to an HD conference.
MaxCPRstIn	Integer	Maximum resolution of a CP conference.
MaxCPRstInCfg	Integer	Configured resolution for a CP conference.
EndpointDispayName	String	The name of the MCU that is displayed on the screen of endpoints that are connecting to the conference.
PALNTSC	NTSC/PAL/AUT O	The video encoding of the RMX.
SeparateMgmtNet	Boolean	Indicates whether management network separation is enabled.
NumPorts	Integer	Total number of ports.
NumVideoPorts	Integer	Number of ports configured for video.

Unified MIB SNMP Fields (Continued)

Name	Туре	Description
ServiceH323	Integer	Indicates the status of H.323 capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
ServiceSIP	Integer	Indicates the status of SIP capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
ServiceISDN	Integer	Indicates the status of SIP capabilities: 1 - The service is enabled and operational. 2 - The service is enabled but is not operational. 3 - The service is disabled.
RsrcAllocMode	Fixed/Flexible	The resource allocation method which determines how the system resources are allocated to the connecting endpoints.
McuSystemStatus	Integer	System State.
FanStatus	Boolean	Status of the hardware fan.
PowerSupplyStatus	Boolean	Status of the power supply.
IntegratedBoardsStatus	Boolean	Status of the integrated boards.
UltraSecureMode	Boolean	Indicates whether the RMX is operating in Ultra Secure Mode.
ChassisTemp	Integer	The temperature of the chasis.
NumPortsUsed	Integer	Number of ports currently in use.
NewCallsPerMinute	Integer	New calls in the last minute.
ScsfNewCallsPerMinute	Integer	Successful new calls in the last minute.
FldNewCallsPerMinute	Integer	Failed new calls in the last minute.
PctScsflNewCalls	Integer	Percentage of new calls in the last minute which were successful.
CallsEndedScsflPerMin	Integer	Number of calls in the last minute which ended with a success code.
CallsEndedFailedPerMin	Integer	Number of calls in the last minute which ended with a failure code.
CallsEndedScsfl	Integer	Number of calls in the last minute which ended with a success code.
CallsEndedFailed	Integer	Number of calls in the last minute which ended with a failure code.
NumActvCnfrncs	Integer	Number of active conferences.

Traps

Three types of traps are sent as follows:

• ColdStart trap. This is a standard trap which is sent when the MCU is reset.

An Example of a ColdStart Trap

coldStart notification received from: 172.22.189.154 at 5/20/2007

7:03:12 PM

Time stamp: 0 days 00h:00m:00s.00th

Agent address: 172.22.189.154 Port: 32774 Transport: IP/UDP

Protocol: SNMPv2c Notification

Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP

Community: public

Enterprise: enterprises.8072.3.2.10

Bindings (3)

 Authentication failure trap. This is a standard trap which is sent when an unauthorized community tries to enter.

An Example of an Authentication Failure Trap

authentication Failure notification received from: 172.22.189.154 at

5/20/2007 7:33:38 PM

Time stamp: 0 days 00h:30m:27s.64th

Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP

Protocol: SNMPv2c Notification

Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP

Community: public

Enterprise: enterprises.8072.3.2.10

Bindings (3)

 Alarm Fault trap. The third trap type is a family of traps defined in the POLYCOM-RMX-MIB file, these traps are associated with the Collaboration Server active alarm and clearance (proprietary SNMP trap).

An Example of an Alarm Fault Trap

rmxFailedConfigUserListInLinuxAlarmFault notification received

from: 172.22.189.154 at 5/20/2007 7:04:22 PM

Time stamp: 0 days 00h:01m:11s.71th

Agent address: 172.22.189.154 Port: 32777 Transport: IP/UDP

Protocol: SNMPv2c Notification

Manager address: 172.22.172.34 Port: 162 Transport: IP/UDP

Community: public

Bindings (6)

Binding #1: sysUpTime.0 *** (timeticks) 0 days 00h:01m:11s.71th

Binding #2: snmpTrapOID.0 *** (oid) rmxFailedConfigUserListInLinuxAlarmFault

Binding #3: rmxAlarmDescription *** (octets) Insufficient resources

Binding #4: rmxActiveAlarmDateAndTime *** (octets)

2007-6-19,16:7:15.0,0:0

Each trap is sent with a time stamp, the agent address, and the manager address.

Status Trap

The MCU sends status traps for the status **MAJOR** - a trap is sent when the card/MCU status is MAJOR. All traps are considered "MAJOR".

RMX MIB entities that do not generate traps.

The following table lists the entities that appear in the RMX MIB of the SNMP that do not generate traps. These traps will be displayed as Faults in the System Alerts pane (at the bottom of the Collaboration Server (RMX) Web Client screen.

SNMP MIB entities that do not generate traps

Key	Description	Comment
5002	Resource process did not receive the Meeting Room list during startup.	
5004	Task terminated	
5008	Low Processing Memory	
5009	Low system Memory	
5010	High system CPU usage	
5014	High CPU utilization	
5016	Process idle	
5107	Failed to open Apache server configuration file	
5108	Failed to save Apache server configuration file	

SNMP MIB entities that do not generate traps (Continued)

Key	Description	Comment
5110	A private version is loaded	
5111	NTP synchronization failure	
5112	Invalid date and time	
5116	Incorrect Ethernet Settings	
5117	Smart Report found errors on hard disk	
5118	Invalid MCU Version	
5150	Music file error	
5205	Unspecified problem	
5207	Unit not responding	
5209	Failed to mount Card folder	
5401	The Log file system is disabled	
5450	Action redirection failure	
5601	Process terminated	
5602	Terminal initiated MCU reset	
5603	User initiated MCU reset	
5604	Internal MCU reset	
5605	MCU reset	
5606	MCU Reset to enable Diagnostics mode	
5607	Startup process failure	
5801	Polycom default User exists. For security reasons, it is recommended to delete this User and create your own User.	Only in non-Ultra Secure Mode
5904	Single clock source	
5950	MCU is not configured for AVF gatekeeper mode	
5652	Hard disk error /AA_HARD_DISK_FAILURE	Not in use
5551	Port configuration modified	Not in use
5011	Used for testing the Active Alarms mechanism	Not in use
5001	License not found	Not in use (Product activation failure is trapped)

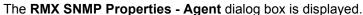
Defining the SNMP Parameters in the Collaboration Server

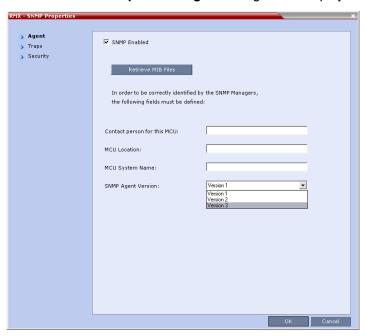
The SNMP option is enabled via the Collaboration Server Web Client application.

The addresses of the Managers monitoring the MCU and other security information are defined in the Collaboration Server Web Client application and are saved on the MCU's hard disk. Only users defined as Administrator can define or modify the SNMP security parameters in the Collaboration Server Web Client application.

To enable SNMP option:

1 In the Collaboration Server Web Client menu bar, click Setup > SNMP.





This dialog box is used to define the basic information for this MCU that will be used by the SNMP system to identify it.

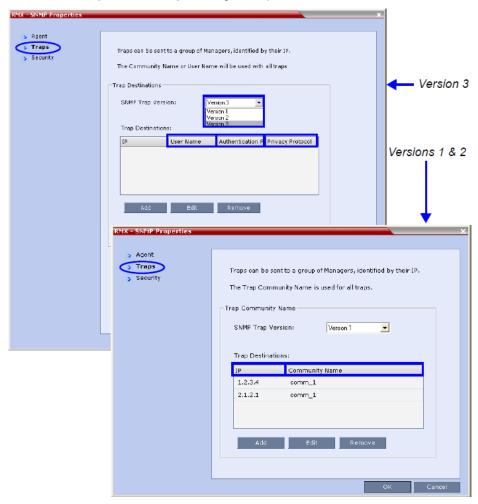
- 2 In the Agent dialog box, click the SNMP Enabled check box.
- 3 Click the Retrieve MIB Files button to obtain a file that lists the MIBs that define the properties of the object being managed.
 - The **Retrieve MIB Files** dialog box is displayed.
- 4 Click the **Browse** button and navigate to the desired directory to save the MIB files.
- 5 Click OK.
 - The path of the selected directory is displayed in the Retrieve MIB Files dialog box.
- 6 Click the Save button.
 - The MIB files are saved to the selected directory.
- 7 Click Close to exit the Retrieve MIB Files dialog box.
- 8 In the Agent dialog box, define the parameters that allow the SNMP Management System and its user to easily identify the MCU.

Collaboration Server-SNMP Properties - Agent Options

Field	Description
Contact person for this MCU	Type the name of the person to be contacted in the event of problems with the MCU.
MCU Location	Type the location of the MCU (address or any description).
MCU System Name	Type the MCU's system name.

9 Click the **Traps** tab.

The **SNMP Properties – Traps** dialog box opens.



Traps are messages sent by the MCU to the SNMP Managers when events such as MCU Startup or Shutdown occur. Traps may be sent to several SNMP Managers whose IP addresses are specified in the **Trap Destinations** box.

10 Define the following parameters:

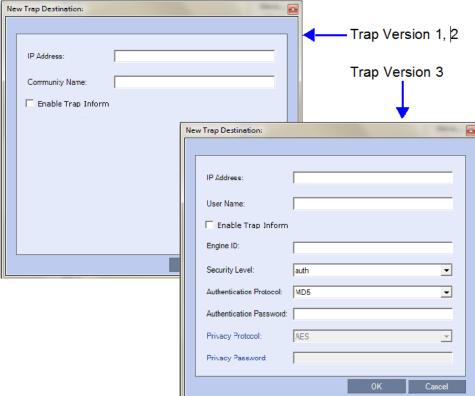
SNMPv3 - Traps

Field	Description			
SNMP Trap Version	Specifies the version, either Version 1 2 or 3 of the traps being sent to the IP Host. Polycom software supports the standard SNMP version 1 and 2 traps, which are taken from RFC 1215, convention for defining traps for use with SNMP. Note: The SNMP Trap Version parameters must be defined identically in the external SNMP application.			
Trap Destination		This box lists the currently defined IP addresses of the Manager terminals to which the message (trap) is sent.		
	IP	Enter the IP address of the SNMP trap recipient.	All Versions	
	Community Name	Enter the Community Name of the manager terminal used to monitor the MCU activity	Version 1 and Version 2	
	User Name	Enter the name of the user who is to have access to the trap.	Version 3	
	Authentication Protocol	Enter the authentication protocol: MD5 or SHA.	_	
	Privacy Protocol	Enter the privacy protocol: DES or AES.	_	
	Engine ID	Enter an Engine ID to be used for both the Agent and the Trap. Default: Empty	_	

¹¹ Click the Add button to add a new Manager terminal.

Depending on the **SNMP Trap Version** selected, one of the two following **New Trap Destination** dialog boxes opens.

New Trap Destination:



12 Define the following parameters:

SNMPv3 - Traps

Field	Description	Version
IP Address	Enter the IP address of the SNMP trap recipient.	
Enable Trap Inform	An Inform is a <i>Trap</i> that requires receipt confirmation from the entity receiving the <i>Trap</i> . If the <i>Engine ID</i> field (<i>Version 3</i>) is empty when <i>Enable Trap Inform</i> has been selected, the <i>Engine ID</i> is set by the <i>Client</i> .	
Community Name	Enter the Community Name of the manager terminal used to monitor the MCU activity	1, 2

SNMPv3 - Traps (Continued)

Field	Description	Version
User Name	Enter the name of the user who is to have access to the trap.	3
Engine ID	Enter an Engine ID to be used for the Trap. This field is enabled when the Enable Trap Inform check box is selected. If the Enable Trap Inform check box is cleared the Engine ID of the Agent is used. The Engine ID is comprised of up to 64 Hexadecimal characters. Default: Empty	-
Security Level	Select a Security Level from the drop-down menu. Range: No Auth, No Priv; Auth, No Priv; Auth, Priv Default: Auth, Priv	-
Authentication Protocol	Enter the authentication protocol: MD5 or SHA. The availability of the MD5 Authentication Protocol as a selectable option is controlled by adding the SNMP_FIPS_MODE System Flag to system.cfg and setting its value. A value of YES means that MD5 will neither be displayed as selectable option nor supported. Range: YES/NO. Default: NO.	-
Authentication Pass	sword	-
Privacy Protocol	Enter the privacy protocol: DES or AES. The availability of the DES Privacy Protocol as a selectable option is controlled by adding the SNMP_FIPS_MODE System Flag to system.cfg and setting its value. A value of YES means that DES will neither be displayed as a selectable option nor supported. Range: YES/NO. Default: NO.	-
Privacy Password		-

13 Type the **IP Address** and the **Community name** of the manager terminal used to monitor the MCU activity, and then click **OK**.

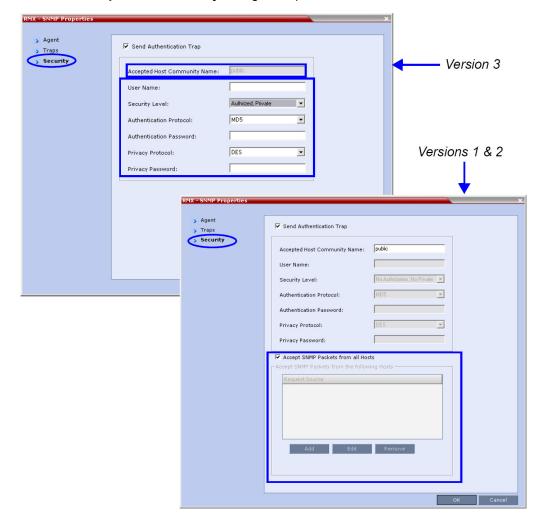
The **Community name** is a string of characters that will be added to the message that is sent to the external Manager terminals. This string is used to identify the message source by the external Manager terminal.

The new IP Address and Community name is added to the Trap Destinations box.

a To delete the IP Address of a Manager terminal, select the address that you wish to delete, and then click the Remove button.

The IP address in the Trap Destinations box is removed.

14 Click the **Security** tab.



The SNMP Properties - Security dialog box opens.

This dialog box is used to define whether the query sent to the MCU is sent from an authorized source. When the "Accept SNMP packets from all Hosts" is disabled, a valid query must contain the appropriate community string and must be sent from one of the Manager terminals whose IP address is listed in this dialog box.

15 Define the following parameters:

SNMP - Security

Field	Description		
Send Authentication Trap	Select this check box to send a message to the SNMP Manager when an unauthorized query is sent to the MCU. When cleared, no indication will be sent to the SNMP Manager.		Versions 1 & 2
Accept Host Community Name	Enter the string added to queries that are sent from the SNMP Manager to indicate that they were sent from an authorized source. Note: Queries sent with different strings will be regarded as a violation of security, and, if the Send Authentication Trap check box is selected, an appropriate message will be sent to the SNMP Manager.		_
Accept SNMP Packets from all Host	Select this option if a query sent from any Manager terminal is valid. When selected, the Accept SNMP Packets from These Hosts option is disabled.		_
Accept SNMP Packets from the following Hosts	Lists specific Manager terminals whose queries will be considered as valid. This option is enabled when the Accept SNMP Packets from any Host option is cleared.		_
User Name	Enter a <i>User Name</i> of up to 48 characters Default : Empty		Version3
Security Level	Select a Security Level from the drop-down menu. Range: No Auth, No Priv; Auth, No Priv; Auth, Priv Default: Auth, Priv		_
Authentication Protocol	Select the authentication protocol Range: MD5, SHA Default: MD5	These fields are enabled if Authentication is selected in the Security Level field.	_
Authentication Password	Enter an Authentication Password. Range: 8 - 48 characters Default: Empty	_	
Privacy Protocol	Select a <i>Privacy Protocol</i> . Range: DES, AES Default: DES	These fields are enabled if Privacy is selected in the Security Level field.	_
Privacy Password	Enter a <i>Privacy Password</i> . Range: 8 - 48 characters Default: Empty	_	
Engine ID	Enter an <i>Engine ID</i> to be used for both the <i>Agent</i> and the <i>Trap</i> . Default: Empty		

¹⁶ To specifically define one or more valid terminals, ensure that the Accept SNMP Packets from any Host option is cleared and then click the Add button.

The Accepted Host IP Address dialog box opens.



17 Enter the IP Address of the Manager terminal from which valid queries may be sent to the MCU, and then click **OK**.

Click the **Add** button to define additional *IP Addresses*.

The IP Address or Addresses are displayed in the Accept SNMP Packets from These Hosts box.



Queries sent from terminals not listed in the *Accept SNMP Packets from These Hosts* box are regarded as a violation of the MCU security, and if the *Send Authentication Trap* check box is selected, an appropriate message will be sent to all the terminals listed in the *SNMP Properties – Traps* dialog box.

18 In the SNMP Properties - Security dialog box, click OK.

Hot Backup

Hot Backup implements a high availability and rapid recovery solution.

Two Collaboration Server's are configured in a *Master/Slave* relationship: the *Master MCU* is active while the *Slave* acts as a passive, fully redundant *Hot Backup* of the *Master MCU*.

All conferencing activities and configuration changes that do not require a *System Reset* are mirrored on the *Slave MCU* five seconds after they occur on the *Master MCU*.

In the event of failure of the *Master MCU*, the *Slave MCU* transparently becomes active and assumes the activities and functions with the backed up settings of the failed *Master MCU*.

In **AVC-based conferencing**, both dial-in and dial-out participants are automatically dialed out and reconnected to their conferences. However, the *Hot Backup* solution is optimized for dial-out participants as all the dial-out numbers are defined in the system and are available for redialing.

In **SVC-based conferencing**, since dial-out is unavailable, SVC-enabled endpoints will have to manually reconnect to the conference.

The following entities are automatically backed up and updated on the Slave MCU:

- Ongoing Conferences
 - Layout
 - Video Force
 - Participant Status (Muted, Blocked, Suspended)
- Reservations
- Meeting Rooms
- Entry Queues
- SIP Factories

- Gateway Profiles
- IVR services (excluding .wav files)
- Recording Link
- Profiles
- IP Network Settings:
 - H.323 settings
 - > SIP settings
 - DNS settings
 - > Fix Ports (TCP, UDP) settings
 - QoS settings

Guidelines for Implementing Hot Backup

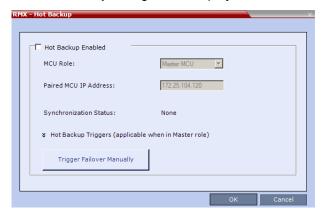
- Both Master and Slave MCUs must have the same software version installed.
- The Users list and Passwords must be the same on both the Master and Slave MCUs.
- There must be connectivity between the Master and Slave MCUs, either on the same network or on different networks connected through routers.
- In the event of failure of the Master MCU the Slave MCU assumes the role of the Master MCU. The Master/Slave relationship is reversed: the Slave, now active, remains the Master and the previous Master MCU, when restarted, assumes the role of Slave MCU.
- No changes to the Slave MCU are permitted while it is functioning as the Hot Backup. Therefore no
 ongoing conferences or reservations can be added manually to the Slave MCU.
- If Hot Backup is disabled, all ongoing conferences and Reservations backed up on the Slave MCU are automatically deleted.
- In Hot Backup configuration, the SIP and H.323 Authentication configuration of the User Name and Password in the IP Network Service Properties - Security tab of the Master Collaboration Server are not backed up in the Slave Collaboration Server.
- Master and Slave initial roles can be reversed only after all ongoing conferences and Reservations are deleted.
- Changes to the Master MCU that require a System Reset can only be made after Hot Backup is disabled.
- Collaboration Server 1500/2000/4000 only: Video/Voice Port Configurations on the Master MCU are not synchronized with the Slave MCU. You must manually set the Video/Voice Port Configurations on both the Master and Slave MCUs to the same level.

Enabling Hot Backup

To enable Hot Backup:

1 On the Collaboration Server menu, click **Setup > Hot Backup**.

The Hot Backup dialog box is displayed.



2 Complete or modify the following fields:

Hot Backup

Field	Description
Hot Backup Enabled	Select this check box to enable <i>Hot Backup</i> .
MCU Role:	This setting determines the role of the MCU in the <i>Hot Backup</i> configuration. Select either Master MCU or Slave MCU from the drop-down menu.
Paired MCU IP Address	 Enter the Control Unit IP Address of the: Slave MCU (if this MCU is the Master) Master MCU (if this MCU is the Slave)
Synchronization Status	 The status of the synchronization between the Master and Slave MCUs in the Hot Backup configuration is indicated as: OK - Hot Backup is functioning normally, and the Master and Slave MCUs are synchronized. Attempting - Hot Backup is attempting to synchronize the Master and Slave MCUs. Fail - A failure occurred while trying to synchronize the paired MCUs. None - Hot Backup has not been enabled.

3 Click OK.

Using Hot Backup Triggers

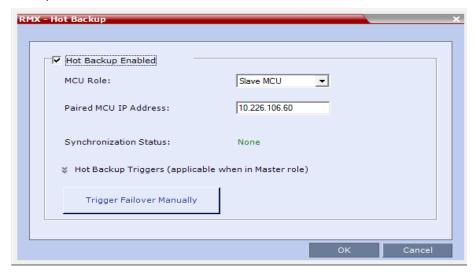
Hot Backup is initiated by the slave MCU on detection of no response from the master MCU on a "Keep Alive" operation. The Hot Backup triggers initiates the Hot Backup swap from Master to Slave when the selected conditions on the Master MCU occur.

Guidelines for Configuring the Hot Backup Triggers

- Hot Backup triggers should be configured on both the Master and Slave MCUs.
- Hot Backup triggers are not synchronized between the Master and Slave MCUs.

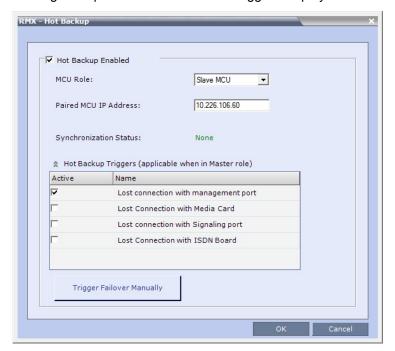
Configuring the Hot Backup Triggers

The Hot Backup triggers are configured in the **Hot Backup** dialog box for the Master MCU when the Hot Backup feature is enabled.



To add the Hot Backup triggers to the Hot Backup configuration:

1 In the Hot Backup dialog box, expand the Trigger Hot Backup Triggers.
A dialog box opens with a list of event triggers displayed.



2 Select the appropriate Hot Backup Triggers check boxes:

Hot Backup Triggers

Hot Backup Trigger	Description
Lost connection with management port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection to the management port is lost on the Master MCU. This trigger is always set.
Lost connection with media port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection with an active media port is lost on the Master MCU.
Lost connection with signalling port	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection with an active signalling port is inactive for a duration of 30 seconds on the Master MCU. A system flag, ETH_INACTIVITY_DURATION, can be added and configured to modify the duration of inactivity of the signalling port. Default value is 30 seconds; Minimum value is 20 seconds.
Lost connection with ISDN card	Initiates the Hot Backup switch from the Master to the Slave MCU when the connection with an ISDN card is disconnected on the Master MCU.

- 3 Alternatively, click the **Trigger Failover Manually** button when you want to trigger the Hot Backup manually and activate the Slave MCU.
 - A confirmation message is displayed.
- 4 Click Yes to continue the Hot Backup process or click No to cancel the Hot Backup process.
- 5 Click OK.

Modifications to the Master MCU Requiring System Reset

Modifications to the configuration of the Master MCU that require a System Reset cannot be performed while Hot Backup is enabled.

To modify the Master MCU configuration:

- 1 Disable the Hot Backup on the Master and Slave MCUs.
- 2 Modify the Master MCUs configuration.
- 3 Reset the Master MCU.
- 4 When the reset is **complete**, enable Hot Backup on the Master and Slave MCUs.
- 5 If required, reset the Slave MCU.

Audible Alarms

In addition to the visual cues used to detect events occurring on the Collaboration Server, an audible alarm can be activated and played when participants request Operator Assistance.

Using Audible Alarms

The Audible Alarm functionality for Operator Assistance requests is enabled for each MCU in either the Collaboration Server Web Client or RMX Manager.

The Audible Alarm played when Operator Assistance is requested is enabled and selected in the **Setup > Audible Alarm > User Customization**.

When the Audible Alarm is activated, the *.wav file selected in the **User Customization** is played, and it is repeated according to the number of repetitions defined in the User Customization.

If more than one Collaboration Server is monitored in the RMX Manager, the Audible Alarm must be enabled separately for each Collaboration Server installed in the site/configuration. A different *.wav file can be selected for each MCU.

When multiple Audible Alarms are activated in different conferences or by multiple MCUs, the Audible Alarms are synchronized and played one after the other. It is important to note that when Stop Repeating Alarm is selected from the toolbar from the Collaboration Server Web Client or RMX Manager, all activated Audible Alarms are immediately halted.

Audible Alarm Permissions

An operator/administrator can configure the Request Operator Assistance audible alarm, however Users with different authorization level have different configuration capabilities as shown in the following table.

Audible Alarm Permissions

Option	Operator	Administrator
User Customization	✓	✓
Download Audible Alarm File		✓
Stop Repeating Alarms	✓	✓

Stop Repeating Message

The Collaboration Server User can stop playing the audible alarm at any time. If more than one audible alarm has been activated, all activated alarms are immediately stopped.

If after stopping the Audible Alarms a new Operator Assistance request event occurs, the audible alarm is re-activated.

To stop the Audible Alarm on the Collaboration Server Client or RMX Manager:

On the Collaboration Server menu, click Setup > Audible Alarms > Stop Repeating Alarm.
 When selected all audible alarms are immediately stopped.

Configuring the Audible Alarms

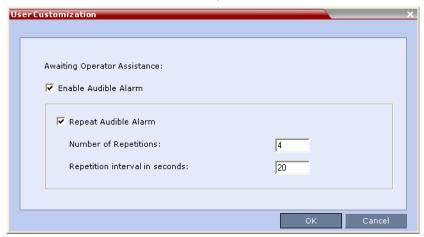
User Customization

The operators and administrators can:

- Enable/Disable the Audible Alarm.
- Select whether to repeat the Audible Alarm.
- Define the number of repetitions and the interval between the repetitions.

To Customize the Audio Alert on the Collaboration Server Client or RMX Manager:

1 On the Collaboration Server menu, click **Setup > Audible Alarms > User Customization**. The **User Customization** window opens.



2 Define the following parameters:

Audible Alarm - User Customization Options

Option	Description
Enable Audible Alarm	Select this check box to enable the Audible Alarm feature and to define its properties.
	When this check box is cleared, the Audible Alarm functionality is disabled.
Repeat Audible Alarm	Select this check box to play the Audible Alarm repeatedly. When selected, it enables the definition of the number of repetitions and the interval between repetitions. When cleared, the Audible Alarm will not be repeated and will be played only once.
Number of Repetitions	Define the number of times the audible alarm will be played. Default number of repetitions is 4.
Repetition interval in seconds	Define the number of seconds that the system will wait before playing the Audible Alarm again. Default interval is 20 seconds.

Click OK.

Replacing the Audible Alarm File

Each Collaboration Server is shipped with a default tone file in *.wav format that plays a specific tone when participants request Operator Assistance. This file can be replaced by a *.wav file with your own recording. The file must be in *.wav format and its length cannot exceed one hour.

Only the User with Administrator permission can download the Audible Alarm file.

To replace the Audio file on the Collaboration Server Client or RMX Manager:

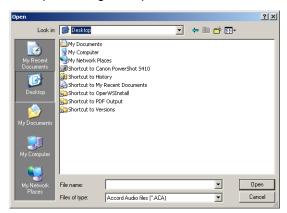
1 On the Collaboration Server menu, click Setup > Audible Alarms > Download Audible Alarm File.

The **Download Audible Alarm File** window opens.



2 Click the **Browse** button to select the audio file (*.wav) to download.

The Open dialog box opens.



- 3 Select the appropriate *.wav file and then click the Open button. The selected file name is displayed in the Install Audible Alarm File dialog box.
- 4 Optional. You can play the selected file or the currently used file by clicking the Play (button as follows:
 - a Click Play Selected File to play a file saved on your computer.
 - b Click Play Collaboration Server File to play the file currently saved on the Collaboration Server.
- 5 In the Download Audible Alarm File dialog box, click OK to download the file to the MCU.

The new file replaces the file stored on the MCU. If multiple Collaboration Servers are configured in the *RMX Manager*, the file must be downloaded to each of the required MCUs separately.

Multilingual Setting

Each supported language is represented by a country flag in the Welcome Screen and can be selected as the language for the Collaboration Server Web Client.

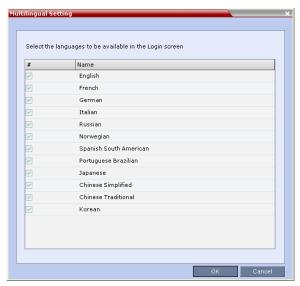
Customizing the Multilingual Setting

The languages available for selection in the Login screen of the Collaboration Server Web Client can be modified using the Multilingual Setting option.

To customize the Multilingual Setting:

1 On the Collaboration Server menu, click Setup > Customize Display Settings > Multilingual Setting.

The **Multilingual Setting** dialog box is displayed.



- 2 Click the check boxes of the languages to be available for selection.
- Click OK.
- 4 Log out from the Collaboration Server Web Client and Log in for the customization to take effect.

Banner Display and Customization

The Login Screen and Main Screen of the Collaboration Server Web Client and the RMX Manager can display informative or warning text banners. These banners can include general information or they can be cautioning users to the terms and conditions under which they may log into and access the system, as required in many secured environments.

Banner display is enabled in the Setup > Customize Display Settings > Banners Configuration.

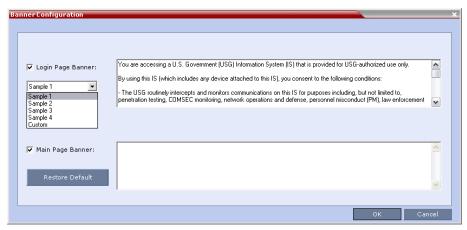


When the **ULTRA_SECURE_MODE** System Flag is set to **YES**, the banners are displayed by default and cannot be disabled. When set to **NO** (default), banner display is according to the check box selection in the *Banners Configuration* dialog box.

The administrator can choose one of four alternative login banners to be displayed. The four alternative banners cannot be modified. A Custom banner (default) can also be defined.

The Main Page Banner is blank and can be defined.

The **Banner Configuration** dialog box allows the administrator to select a **Login Banner** from a drop-down menu.



One of the following Login Banners can be selected:

- Non-Modifiable Banners
 - > Sample 1
 - > Sample 2
 - ➤ Sample 3
 - > Sample 4
- Modifiable Banner
 - Custom (Default)

Guidelines

- The Login Banner cannot be disabled when the Collaboration Server is in Ultra Secure Mode.
- The Login Banner must be acknowledged before the user is permitted to log in to the system.
- If a Custom banner has been created, and the user selects one of the alternative, non-modifiable banners the Custom banner not deleted.
- The Custom Login Banner may contain up to 1300 characters.
- An empty Login Banner is not allowed.
- Any attempt to modify a non-modifiable banner results in it automatically being copied to the Custom banner.

Non-Modifiable Banner Text

Sample 1 Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Sample 2 Banner

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users also may be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Sample 3 Banner

You are about to access a system that is intended for authorized users only. You should have no expectation of privacy in your use of this system. Use of this system constitutes consent to monitoring, retrieval, and disclosure of any information stored within the system for any purpose including criminal prosecution.

Sample 4 Banner

This computer system including all related equipment, network devices (specifically including Internet access), is provided only for authorized use. All computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized personnel and their entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information including personal information, placed on or sent over this system may be monitored. Use of this system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of any such unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

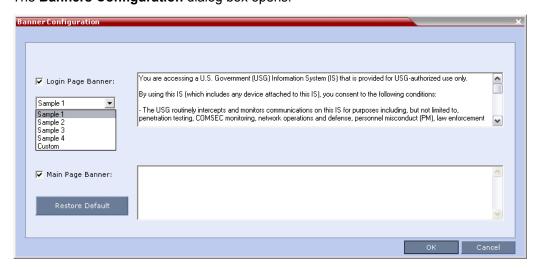
Customizing Banners

The Login and Main Screen banners can be customized to display conference information, assistance information or warning text as required in the Ultra Secure Mode.

To customize the banners:

1 In the Collaboration Server menu, click Setup > Customize Display Settings > Banners Configuration.

The Banners Configuration dialog box opens.



2 Customize the banners by modifying the following fields:

Banner Configuration

	Description		
Field	Check Box	Text Field	Restore Default Button
Login Page Banner Main Page Banner	Select or clear the check box to enable or disable the display of the banner. Note: Banner display cannot be disabled in when the ULTRA SECURE_MODE flag is set to YES.	Edit the text in this field to meet local requirements: Banner content is multilingual and uses Unicode, UTF-8 encoding. All text and special characters can be used. Maximum banner size is 100KB. The banner may not be left blank when the ULTRA SECURE_MODE flag is set to YES.	Click the button to restore the default text to the banner

3 Click the OK button.

Banner Display

Login Screen Banner

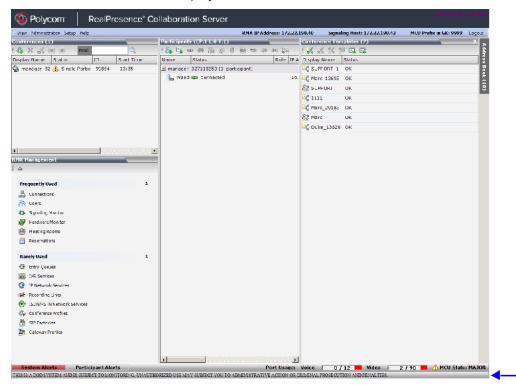
The Login screen banner can display any text, for example the terms and conditions for system usage. The default text is that required in *Ultra Secure Mode*. The user must acknowledge that the information was read and click the **Accept** button to proceed to the Login screen as shown in the following screen:



When the Collaboration Server is configured to work in Ultra Secure Mode, such as Maximum Security Environments, the display banner includes the terms and conditions for system usage as detailed in the default text: contained in Sample Banner 1.

Main Screen Banner

The Main Screen banner is displayed at the bottom of the screen:



When the Collaboration Server is configured to work in Ultra Secure Mode, such as the Maximum Security environment, the display banner includes the following default text:

Banner

THIS IS A DOD SYSTEM AND IS SUBJECT TO MONITORING, UNAUTHORIZED USE MAY SUBJECT YOU TO ADMINISTRATIVE ACTION OR CRIMINAL PROSECUTION AND PENALTIES.

Software Management

The Software Management menu is used to backup and restore the Collaboration Server's configuration files and to download MCU software.

Backup and Restore Guidelines

- Direct access to the Collaboration Server file system is disabled in both Ultra Secure Mode and standard security mode.
- System Backup can only be performed by an administrator.
- The System Backup procedure creates a single backup file that can be viewed or modified only by developers.
- A System Backup file from one system can be restored on another system.
- To ensure file system consistency, do not perform any configuration changes as the system does not suspended them during the backup procedure.
- The following parameters, settings and files are backed up:
 - MCMS configuration files (/mcms/Cfg):
 - Network and service configurations,
 - Rooms,
 - Profiles
 - Reservations
 - System Flags
 - Resource Allocation
 - IVR messages, music
 - Collaboration Server Web Client user setting fonts, windows
 - Collaboration Server Web Client global settings notes, address book, language
 - Private keys and certificates (TLS)
 - Conference participant settings
 - Operation DB (administrator list)
 - SNMP settings
 - > Time configuration
- CDR files are not included in the backup process and should be backed up manually by saving the CDR files to a destination device.

Using Software Management

To backup configuration files:

1 On the Collaboration Server menu, click **Administration > Software Management > Backup Configuration**.

The Backup Configuration dialog box opens.



- 2 Click the Browse button. The Browse To File dialog box opens.
- 3 Select the Backup Directory Path and then click Backup.



When the Collaboration Server system backs up the current configuration, if any changes occur immediately or during the request, then additional changes are not registered.

To restore configuration files:

- 1 On the Collaboration Server menu, click **Administration > Software Management > Restore Configuration**.
- **2 Browse** to the *Restore Directory Path* where the backed up configuration files are stored and then click **Restore**.

To download MCU software files:

- 1 On the Collaboration Server menu, click Administration > Software Management > Software Download.
- 2 Browse to the *Install Path* and then click **Install**.

Ping the Collaboration Server

The Ping administration tool enables the Collaboration Server Signaling Host to test network connectivity by Pinging IP addresses.

Guidelines

- The IP addressing mode can be either IPv4 or IPv6.
- Both explicit IP addresses and Host Names are supported.
- The Collaboration Server Web Client blocks any attempt to issue another Ping command before the current Ping command has completed. Multiple Ping commands issued simultaneously from multiple Collaboration Server Web Clients are also blocked.

Using Ping

To Ping a network entity from the Collaboration Server:

1 On the Collaboration Server menu, click Administration > Tools > Ping. The Ping dialog box is displayed:



2 Modify or complete the following fields:

Ping Parameters

Field	Description
IP Version	Select IPv4 or IPv6 from the drop-down menu.
Host Name or Address	Enter the Host Name or IP Address of the network entity to be Pinged.

3 Click the Ping button.

The Ping request is sent to the Host Name or IP Address of the Collaboration Server entity.

The Answer is either:

- > OK, or
- > FAILED

Notification Settings

The Collaboration Server can display notifications when:

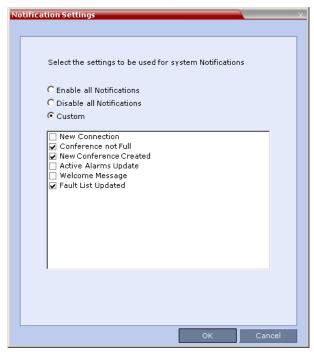
- A new Collaboration Server user connects to the MCU.
- A new conference is started.
- Not all defined participants are connected to the conference or when a single participant is connected.
- A change in the MCU status occurs and an alarm is added to the alarms list.

A welcome message is displayed to the Collaboration Server user upon connection.



To configure the notifications:

1 On the Collaboration Server menu, select Setup > Notification Settings. The Notification Settings dialog box is displayed.



The following notification options are displayed.

Notification Settings Parameters

Field	Description
New Connection	Notification of a new user/administrator connecting to the Collaboration Server.
New Conference Created	New conference has been created.

Notification Settings Parameters (Continued)

Field	Description
Conference Not Full	The conference is not full and additional participants are defined for the conference.
Welcome Message	A welcome message after user/administrator logon.
Active Alarms Update	Updates you of any new alarm that occurred.
Fault List Updated	Updates you when the faults list is updated (new faults are added or existing faults are removed).

- 2 Enable/Disable All Notifications or Custom to select specific notifications to display.
- 3 Click OK.

Logger Diagnostic Files

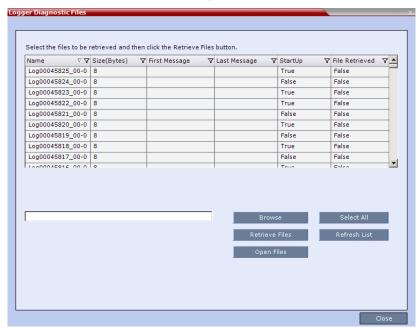
The Logger utility is a troubleshooting tool that continually records MCU system messages and saves them to files in the MCU hard drive. For each time interval defined in the system, a different data file is created. The files may be retrieved from the hard drive for off-line analysis and debugging purposes.

The Logger utility is activated at the MCU startup. The Logger is disabled when the MCU is reset manually or when there is a problem with the Logger utility, e.g. errors on the hard drive where files are saved. In such cases, data cannot be retrieved.

When the MCU is reset via the Collaboration Server, the files are saved on the MCU hard drive.

To access the Logger Diagnostic Files:

On the Collaboration Server menu, click Administration > Tools > Logger Diagnostic Files.



The following tasks can be performed:

Diagnostic File Button Options

Button	Description
Refresh List	Refreshes the list and adds newly generated logger files.
Select All	Selects all the logger files listed.
Browse	Selects the destination folder for download.
Retrieve Files	Saves files to the destination folder.

When retrieved, the log file name structure is as follows:

• Sequence number (starting with 1)

- Date and Time of first message
- Date and Time of last message
- File size
- Special information about the data, such as Startup

File name structure:

Log SNxxxxxxxx FMDddmmyyy FMThhmm LMDddmmyyyy LMThhmm SZxxxxxxxx SUY.log

File name format:

- SN = Sequence Number
- FM = First Message, date and time
- LM = Last Message, date and time
- SZ = Size
- SU = Startup (Y/N) during the log file duration

Example:

Log SN000000002 FMD06032007 FMT083933 LMD06032007 LMT084356 SZ184951 SUY.log.

To Retrieve the Logger Files:

- 1 Select the log files to retrieve. Multiple selections of files are enabled using standard Windows conventions.
- 2 In the Logger Diagnostic Files dialog box, click the Browse button.
- 3 In the **Browse for Folder** window, select the directory location to save the Logger files and click **OK**. You will return to the **Logger Diagnostic Files** dialog box.

Logger Diagnostic Files Select the files to be retrieved and then click the Retrieve Files button. ∇ ▼ Size(Bytes) ▼ First Message ▼ File Retrieved ▼ ▲ Log00045775_10-0 1019595 10 June 2012 04:09: 10 June 2012 04:2 False Log00045774_10-0 1016689 10 June 2012 03:54: 10 June 2012 04:0 False False Log00045773_10-0 1018764 10 June 2012 03:40: 10 June 2012 03:5 False 10 June 2012 03:25: 10 June 2012 03:4 Log00045772_10-0 1019097 False Log00045771_10-0 1017513 10 June 2012 03:10: 10 June 2012 03:2 False Log00045770_09-0 1043047 10 June 2012 02:05: 10 June 2012 03:1 False False Log00045769_09-0 1017436 10 June 2012 01:51: 10 June 2012 02:0 False False Retrieving RealPresence Collaboration ...×

4 Click the Retrieve Files button.

The log files (in *.txt format) are saved to the defined directory and a confirmation caption box is displayed indicating a successful retrieval of the log files.

Viewing the Logger Files:

To analyze the log files generated by the system, open the retrieved *.txt files in any text editor application, i.e. Notepad, Textpad or MS Word.

- 1 Using Windows Explorer, browse to the directory containing the retrieved log files.
- **2** Use any text editor application to open the log file(s).

Information Collector

Standard Security Mode

The Information Collector comprehensively attains all information from all the MCU internal entities for data analysis. That data, stored in a central repository, is logged from the following system components:

- · System Log Files
- CDR
- OS (Core dumps, CFG DNS, DHCP, NTP, kernal state, event logs
- Signaling Trace files (H.323 & SIP)
- · Central Signaling logs
- · Processes internal state and statistics

- · Full faults
- · Apache logs
- · CFG directory (without IVR)
- · Cards info: HW version, state and status
- · SW version number
- •

The data collected is saved into a single compressed file containing all the information from each system component in its relative format (.txt, .xml, etc...). In case the disk is malfunctioning, the file will be written to the RAM (involves only a small amount of information where the RAM size is 1/2 a gigabyte). The zipped file (info.tgz) can be opened with the following applications: WinRAR and WinZip. The entire zipped file is then sent to Polycom's Network Systems Division for analysis and troubleshooting.

Ultra Secure Mode

The Information Collector logs information from the Collaboration Server's Network Intrusion Detection System (NIDS), saving it into a compressed disk file. (If the disk malfunctions, the file is written to RAM.) The zipped file (info.tgz) can be opened with either WinRAR or WinZip. The entire zipped file can be sent to Polycom for analysis.

Network Intrusion Detection System (NIDS)

The Collaboration Server system uses iptables for access control. For each different kind of packet processing, there is a table containing chained rules for the treatment of packets. Every network packet arriving at or leaving from the Collaboration Server must pass the rules applicable to it.

Depending on the nature of the suspect packets, the rules may reject, drop, or limit their arrival rate (dropping the rest).

The Collaboration Server maintains a log that includes all unpermitted access attempts blocked by the fire wall.

Unpermitted access includes:

- Access to ports which are not opened on the Collaboration Server.
- Invalid access to open ports.

Using the Information Collector

When the Information Collector is used the following steps are performed:

- Step 1: Creating the Information Collector file.
- Step 2: Saving the Information Collector file.
- Step 3: Viewing the information in the Information Collector file.

Step 1: Creating the Information Collector Compressed File

To create the compressed file:

1 In the Collaboration Server menu, click **Administration > Tools > Information Collector**. The **Information Collector** dialog box is displayed.

Information Collector - Standard Security Mode



Information Collector - Ultra Secure Mode



- 2 In the **From Date** and **Until Date** fields, use the arrow keys to define the date range of the data files to be included in the compressed file.
- 3 In the From Time and Until Time fields, use the arrow keys to define the time range of the data files to be included in the compressed file.



If logs are being collected in order to troubleshoot a specific issue, it is important that the date and time range include the time and date in which the issue occurred. The default date and time ranges may not be sufficient.

For example, if a specific issue occurred on October 1, 2013 at 12:15, the *From Date* and *Until Date* should be October 1, 2013, the *From Time* should be around 12:10, and the *Until Time* should be around 12:20.

- 4 Select check boxes of the information to be collected.
- In the **Export Path** field, click the **Browse** button and navigate to the directory path where the compressed file is to be saved.
- 6 Click the Collect Information button.

A progress indicator is displayed in the **Information Collector** dialog box while the file is being created.

Step 2: Saving the Compressed File

- 1 The compressed file is automatically saved in the directory selected in the *Information Collector* dialog box. The file is named **info.tgz**.
 - A success information box is displayed.
- 2 Click the **OK** button.

Step 3: Viewing the Compressed File

The compressed file is saved in .tgz format and can be viewed with any utility that can open files of that format, for example WinRAR® 3.80.

To view the compressed file:

- 1 Navigate to the directory on the workstation in which the file was saved.
- 2 Double click the **info.tgz** file to view the downloaded information.



Some browsers save the file as *info.gz* due to a browser bug. If this occurs, the file must be manually renamed to *info.tgz* before it can be viewed.

Auditor

An Auditor is a user who can view Auditor and CDR files for system auditing purposes.



The Auditor user must connect to the Collaboration Server using the Collaboration Server Web Client only.

The Event Auditor enables administrators and auditors to analyze configuration changes and unusual or malicious activities in the Collaboration Server system.

Auditor operates in real time, recording all administration activities and login attempts from the following Collaboration Server modules:

- Control Unit
- Shelf Manager

For a full list of monitored activities, see Audit Events.

The Auditor must always be active in the system. A System Alert is displayed if it becomes inactive for any reason.

The Auditor tool is composed of the Auditor Files and the Auditor File Viewer that enables you to view the Auditor Files.



Time stamps of Audit Events are GMT.

Auditor Files

All audit events are saved to a buffer file on hard disk in real time and then written to a file on hard disk in XML in an uncompressed format.

A new current auditor event file is created when:

- · the system is started
- the size of the current auditor event file exceeds 2 MB
- the current auditor event file's age exceeds 24 hours

Up to 1000 auditor event files are stored per Collaboration Server. These files are retained for at least one year and require 1.05 GB of disk space. The files are automatically deleted by the system (oldest first) when the system reaches the auditor event file limit of 1000.

A System Alert is displayed with Can't store data displayed in its Description field if:

- the system cannot store 1000 files
- the Collaboration Server does not have available disk space to retain files for one year

Audit Event Files are retained by the Collaboration Server for at least 1 year. Any attempt to delete an audit event file that is less than one year old raises a System Alert with File was removed listed in the Description field.

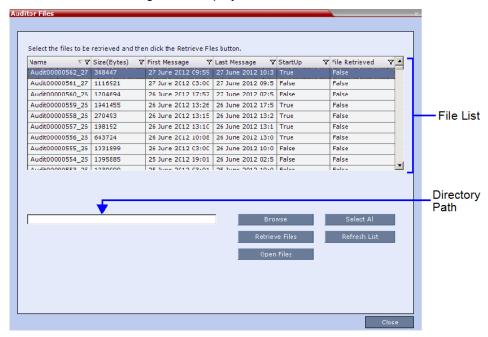
Using the Restore Factory Defaults of the System Restore procedure erases Audit Files.

Retrieving Auditor Files

You can open the Auditor file directly from the Auditor Files list or you can retrieve the files and save them to a local workstation.

To access Auditor Files:

On the Collaboration Server menu, click Administration > Tools > Auditor Files.



The **Auditor Files** dialog box is displayed.

The Auditor Files dialogue box displays a file list containing the following file information:

- Name
- ➤ Size (Bytes)
- > First Message date and time of the first audit event in the file
- Last Message date and time of the last audit event in the file
- StartUp:
 - ♦ True file was created when the system was started
 - ♦ False file was created when previous audit event file reached a size of 2 MB or was more than 24 hours old
- > File Retrieved:
 - True file was previously retrieved.
 - ♦ False file was never previously retrieved.

The order of the *Auditor Files* dialog box field header columns can be changed and the fields can be filtered to enable searching.

For more information, see Auditor File Viewer.

To retrieve files for storage on a workstation:

- 1 Click Browse and select the folder on the workstation to receive the files and then click OK.
 The folder name is displayed in the directory path field.
- 2 Select the file(s) to be retrieved by clicking their names in the file list or click **Select All** to retrieve all the files. (Windows multiple selection techniques can be used.)

3 Click Retrieve Files.

The selected files are copied to the selected directory on the workstation.

To open the file in the Auditor File Viewer:

• Double-click the file.

Auditor File Viewer

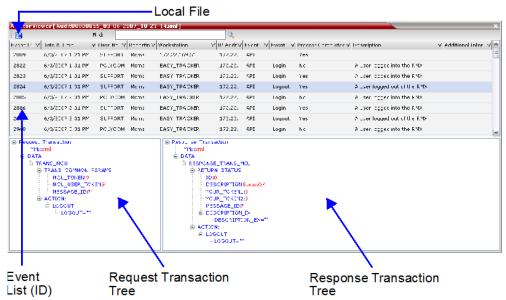
The Auditor File Viewer enables Auditors and Administrators to view the content of and perform detailed analysis on auditor event data in a selected Auditor Event File.

You can view an Auditor Event File directly from the Auditor Files list or by opening the file from the Auditor File Viewer.

To open the Auditor File Viewer from the Administration Menu:

1 On the Collaboration Server menu, click Administration > Tools > Auditor File Viewer. The Auditor File Viewer is displayed.

If you previously double clicked an Auditor Event File in the Auditor Files list, that file is automatically opened.



The following fields are displayed for each event:

Auditor Event Columns

Field	Description
Event ID	The sequence number of the event generated by the Collaboration Server.
Date & Time	The date and time of the event taken from the <i>Collaboration Server's Local Time</i> setting.
User Name	The Username (Login Name) of the user who triggered the event.
Reporting Module	The Collaboration Server system internal module that reported the event: MCMS MPL Central Signaling MPL Simulation Collaboration Server Web Client CM Switch Shelf Management ART Video Card Manager RTM MUX
Workstation	The name (alias) of the workstation used to send the request that triggered the event.

Auditor Event Columns (Continued)

Field	Description
IP Address (Workstation)	The IP address of the workstation used to send the request that triggered the event.
Event Type	Auditor events can be triggered by: API HTTP Collaboration Server Internal Event
Event	The process, action, request or transaction that was performed or rejected. POST:SET transactions (API) Configuration changes via XML (API) Login/Logout (API) GET (HTTP) PUT (HTTP) MKDIR (HTTP) RMDIR (HTTP) Startup (Collaboration Server Internal Event) Shutdown (Collaboration Server Internal Event) Reset (Collaboration Server Internal Event) Enter Diagnostic Mode (Collaboration Server Internal Event) IP address changes via USB (Collaboration Server Internal Event)
Process Completed	Status of the process, action, request or transaction returned by the system: • Yes – performed by the system. • No – rejected by the system.
Description	A text string describing the process, action, request or transaction.
Additional Information	An optional text string describing the process, action, request or transaction in additional detail.

The order of the Auditor File Viewer field header columns can be changed and the fields can be sorted and filtered to facilitate different analysis methods.

2 In the event list, click the events or use the keyboard's Up-arrow and Down-arrow keys to display the Request Transaction and Response Transaction XML trees for each audit event.

The transaction XML trees can be expanded and collapsed by clicking the expand (\boxdot) and collapse (\boxdot) buttons.

To open an auditor event file stored on the workstation:

- 1 Click the **Local File** button () to open the *Open* dialogue box.
- 2 Navigate to the folder on the workstation that contains the audit event file.
- 3 Select the audit event file to be opened.
- 4 Click Open.

The selected file is opened in the Auditor Viewer.

Audit Events

Alerts and Faults

NTP synchronization failure.

Alerts and Faults that are recorded by the Auditor.

Alerts and Faults recorded by the Auditor

Event
Attempt to exceed the maximum number of management session per user
Attempt to exceed the maximum number of management sessions per system
Central Signaling indicating Recovery status.
Failed login attempt
Failed to open Apache server configuration file.
Failed to save Apache server configuration file.
Fallback version is being used.
File system scan failure.
File system space shortage.
Internal MCU reset.
Internal System configuration during startup.
Invalid date and time.
Invalid MCU Version.
IP addresses of Signaling Host and Control Unit are the same.
IP Network Service configuration modified.
IP Network Service deleted.
Login
Logout
Management Session Time Out
MCU Reset to enable Diagnostics mode.
MCU reset.
Music file error.
New activation key was loaded.
New version was installed.
NTD are about a failure

Alerts and Faults recorded by the Auditor (Continued)

Event

Polycom default User exists.

Private version is loaded.

Restoring Factory Defaults.

Secured SIP communication failed.

Session disconnected without logout

SSH is enabled.

System Configuration modified.

System is starting.

System Resets.

TCP disconnection

Terminal initiated MCU reset.

The Log file system is disabled.

The software contains patch(es).

USB key used to change system configuration.

User closed the browser

User initiated MCU reset.

Transactions

Transactions that are recorded by the Auditor.

Transactions recorded by the Auditor

Transaction

TRANS_CFG:SET_CFG

TRANS_IP_SERVICE:DEL_IP_SERVICE

TRANS_IP_SERVICE:NEW_IP_SERVICE

TRANS_IP_SERVICE:SET_DEFAULT_H323_SERVICE

TRANS_IP_SERVICE:SET_DEFAULT_SIP_SERVICE

TRANS_IP_SERVICE:UPDATE_IP_SERVICE

TRANS_IP_SERVICE:UPDATE_MANAGEMENT_NETWORK

TRANS_ISDN_PHONE:ADD_ISDN_PHONE

TRANS_ISDN_PHONE:DEL_ISDN_PHONE

Transactions recorded by the Auditor (Continued)

TRANS_ISDN_PHONE:UPDATE_ISDN_PHONE TRANS_ISDN_SERVICE:DEL_ISDN_SERVICE TRANS_ISDN_SERVICE:NEW_ISDN_SERVICE TRANS_ISDN_SERVICE:SET_DEFAULT_ISDN_SERVICE TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE TRANS_MCU:BEGIN_RECEIVING_VERSION TRANS_MCU:COLLECT_INFO TRANS_MCU:CREATE_DIRECTORY TRANS_MCU:CREATE_DIRECTORY TRANS_MCU:FINISHED_TRANSFER_VERSION TRANS_MCU:LOGIN TRANS_MCU:LOGOUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:RESET TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_TIME TRANS_MCU:UPDATE_KEY_CODE TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:DELETE_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	Transaction
TRANS_ISDN_SERVICE:NEW_ISDN_SERVICE TRANS_ISDN_SERVICE:SET_DEFAULT_ISDN_SERVICE TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE TRANS_MCU:BEGIN_RECEIVING_VERSION TRANS_MCU:COLLECT_INFO TRANS_MCU:CREATE_DIRECTORY TRANS_MCU:FINISHED_TRANSFER_VERSION TRANS_MCU:LOGIN TRANS_MCU:LOGUT TRANS_MCU:LOGOUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RENAME TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_TIME TRANS_MCU:SET_TIME TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR.SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_ISDN_PHONE:UPDATE_ISDN_PHONE
TRANS_ISDN_SERVICE:SET_DEFAULT_ISDN_SERVICE TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE TRANS_MCU:BEGIN_RECEIVING_VERSION TRANS_MCU:COLLECT_INFO TRANS_MCU:CREATE_DIRECTORY TRANS_MCU:FINISHED_TRANSFER_VERSION TRANS_MCU:LOGIN TRANS_MCU:LOGUT TRANS_MCU:LOGUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RESET TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:DPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_ISDN_SERVICE:DEL_ISDN_SERVICE
TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE TRANS_MCU:BEGIN_RECEIVING_VERSION TRANS_MCU:COLLECT_INFO TRANS_MCU:CREATE_DIRECTORY TRANS_MCU:FINISHED_TRANSFER_VERSION TRANS_MCU:LOGIN TRANS_MCU:LOGOUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:RESET TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:SET_TIME TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_ISDN_SERVICE:NEW_ISDN_SERVICE
TRANS_MCU:BEGIN_RECEIVING_VERSION TRANS_MCU:COLLECT_INFO TRANS_MCU:CREATE_DIRECTORY TRANS_MCU:FINISHED_TRANSFER_VERSION TRANS_MCU:LOGIN TRANS_MCU:LOGOUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RESET TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR	TRANS_ISDN_SERVICE:SET_DEFAULT_ISDN_SERVICE
TRANS_MCU:COLLECT_INFO TRANS_MCU:CREATE_DIRECTORY TRANS_MCU:FINISHED_TRANSFER_VERSION TRANS_MCU:LOGIN TRANS_MCU:LOGOUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RESET TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR	TRANS_ISDN_SERVICE:UPDATE_ISDN_SERVICE
TRANS_MCU:CREATE_DIRECTORY TRANS_MCU:FINISHED_TRANSFER_VERSION TRANS_MCU:LOGIN TRANS_MCU:LOGOUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RENAME TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:SUTURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:BEGIN_RECEIVING_VERSION
TRANS_MCU:FINISHED_TRANSFER_VERSION TRANS_MCU:LOGIN TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RENAME TRANS_MCU:RESET TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR	TRANS_MCU:COLLECT_INFO
TRANS_MCU:LOGIN TRANS_MCU:LOGOUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RENAME TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR	TRANS_MCU:CREATE_DIRECTORY
TRANS_MCU:LOGOUT TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RENAME TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR	TRANS_MCU:FINISHED_TRANSFER_VERSION
TRANS_MCU:REMOVE_DIRECTORY TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RENAME TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_OPERATOR:NEW_OPERATOR	TRANS_MCU:LOGIN
TRANS_MCU:REMOVE_DIRECTORY_CONTENT TRANS_MCU:RENAME TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:LOGOUT
TRANS_MCU:RENAME TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:REMOVE_DIRECTORY
TRANS_MCU:RESET TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:REMOVE_DIRECTORY_CONTENT
TRANS_MCU:SET_PORT_CONFIGURATION TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:RENAME
TRANS_MCU:SET_RESTORE_TYPE TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:RESET
TRANS_MCU:SET_TIME TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:SET_PORT_CONFIGURATION
TRANS_MCU:TURN_SSH TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:SET_RESTORE_TYPE
TRANS_MCU:UPDATE_KEY_CODE TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:SET_TIME
TRANS_OPERATOR:CHANGE_PASSWORD TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:TURN_SSH
TRANS_OPERATOR:DELETE_OPERATOR TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_MCU:UPDATE_KEY_CODE
TRANS_OPERATOR:NEW_OPERATOR TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_OPERATOR:CHANGE_PASSWORD
TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN	TRANS_OPERATOR:DELETE_OPERATOR
	TRANS_OPERATOR:NEW_OPERATOR
TRANS SNMP:UPDATE	TRANS_RTM_ISDN_SPAN:UPDATE_RTM_ISDN_SPAN
	TRANS_SNMP:UPDATE

ActiveX Bypass

At sites that, for security reasons, do not permit Microsoft® ActiveX® to be installed, the MSI (Windows Installer File) utility can be used to install .NET Framework and .NET Security Settings components on workstations throughout the network.

All workstation that connect to Collaboration Server systems must have both.NET Framework and .NET Security Settings running locally. These components are used for communication with the Collaboration Server and can only be installed on workstations by users with administrator privileges.

The MSI utility requires the IP addresses of all the Collaboration Server systems (both control unit and Shelf Management IP addresses) that each workstation is to connect to.

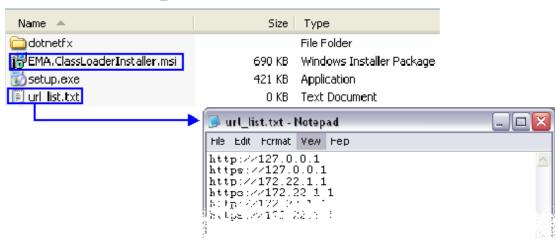
If the IP address of the any of the target Collaboration Servers is changed, the ActiveX components must be reinstalled.

Installing ActiveX

To install ActiveX components on all workstations in the network:

- 1 Download the MSI file **EMA.ClassLoaderInstaller.msi** from the Polycom Resource Center. The MSI file contains installation scripts for both .NET Framework and .NET Security Settings.
- 2 Create a text file to be used during the installation containing the IP addresses of all the Collaboration Server systems (both control unit and Shelf Management IP addresses) that each workstation in the network is to connect to.

The file must be named url_list.txt and must be saved in the same folder as the downloaded MSI file.



3 Install the ActiveX components on all workstations on the network that connect to Collaboration Server systems.

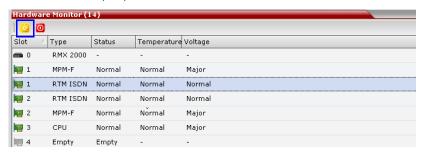
The installation is done by the network administrator using a 3rd party network software installation utility and is transparent to all other users.

Resetting the Collaboration Server

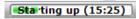
System Reset saves system configuration changes and restarts the system with the latest settings.

To reset the RMX:

- 1 In the RMX Management pane, click the Hardware Monitor button.
 The Hardware Monitor pane is displayed.
- 2 Click the Reset (button.



When the Collaboration Server system is reset, during Collaboration Server startup the Progress Bar appears at the bottom of the Collaboration Server *Status* pane, displaying the amount of time remaining for the reset process to complete:



The Startup progress is also indicated by a green bar moving from left to right.

The duration of the *Startup* depends on the type of activity that preceded the MCU reset. For example: Fast Configuration Wizard, New Version installation, Version Upgrade, Restore Last Configuration etc.



When resetting the Collaboration Server from the Hardware Monitor, sometimes SIP endpoints may remain connected, although the conference ended.

1



These instructions are applicable to the RealPresence Collaboration Server Virtual Edition only.



These instructions are applicable to the RealPresence Collaboration Server 800s only.

System Configuration Flags

The system's overall behavior can be configured by modifying the default values of the System Flags.



For flag changes (including deletion) to take effect, the MCU must be reset.

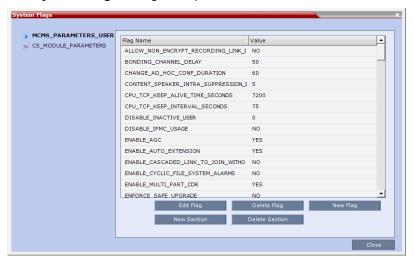
The following **System Flags** do not require an MCU reset:

- IVR_MESSAGE_VOLUME
- IVR_MUSIC_VOLUME
- IVR_ROLL_CALL_VOLUME
- ENABLE_SELECTIVE_MIXING

Modifying System Flags

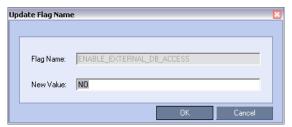
To modify system flags:

1 On the Collaboration Server menu, click Setup > System Configuration. The System Flags dialog box opens.



- 2 In the MCMS_PARAMETERS_USER tab, the flags listed in the MCMS_PARAMETERS_USER Flags table can be modified.
- 3 To modify a flag value, double-click or select the flag and click Edit Flag.

4 In the **New Value** field, enter the flag's new value.



- 5 Click **OK** to close the **Update Flag** dialog box.
- 6 Repeat steps 2-4 to modify additional flags.
- 7 Click **OK** to close the **System Flags** dialog box.



For flag changes (including deletion) to take effect, reset the MCU. For more information see Resetting the Collaboration Server.

MCMS_PARAMETERS_USER Flags

Flag	Description
ALLOW_NON_ENCRYPT_ PARTY_IN_ENCRYPT_CONF	If YES, allows non-encrypted participants to connect to encrypted conferences. Default: NO Note: From Version 7.6.1, this flag is replaced by the Encryption option Encrypt when Possible in the conference Profile - Advanced dialog box. Flag setting is ignored.
ALLOW_NON_ENCRYPT_ RECORDING_LINK_IN_ ENCRYPT_CONF	When set to NO (default), the Recording Link inherits the encryption settings of the conference. If the conference is encrypted, the recording link will be encrypted. When set to YES , it disables the encryption of the recording link, regardless of the Encryption settings of the conference and RSS recorder.
AUTHENTICATE_USER	This flag is not supported from Version 7.7. If the external database application is to be used to verify that operators are authorized to log in to the MCU, set the value of this flag to YES. If the value of this flag is set to NO, the MCU database is used to verify that operators are authorized to log in to the MCU. Note: If the flag is set to YES, the flow is first to look in the internal DB and then go out to the external one. Flags for SE200 need to be added manually.

Flag	Description
BONDING_CHANNEL_DELAY (ISDN)	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. When connecting a bonding group, this is the delay (number of 1/100
	seconds) between dialing attempts to connect sequential channels. The channel per second connection performance of ISDN switches can vary and can cause timing issues that result in bonding channel disconnection. Default: 6
CHANGE_AD_HOC_CONF_ DURATION	The duration of an ad-hoc conference* can be configured on a system level by setting the flag to one of the following values (in minutes): 60 (default), 90 , 180 and 270 .
	* An ad-hoc conference is automatically created when the participant dials into an Ad-hoc Entry Queue and enters a conference ID that is not being used by any other conferencing entity. It is based on the Conference Profile assigned to the EQ.
CHECK_ARPING	This flag is not supported from Version 7.7. Disables Duplicate Address Detection and should be configured according to local site policy. When set to YES , Duplicate Address Detection is enabled in for both IPv4 and IPv6. When set to NO , Duplicate Address Detection is disabled for both IPv4 and IPv6. When using IPv6, ICMPv6 type 135 packets are also disabled.
CONTENT_SLAVE_LINKS_INTR A_SUPPRESSION_IN_ SECONDS	Defines the interval, in seconds, during which the Collaboration Server is allowed to forward an Intra Request received from any of the Slave Cascading Links. The Slave Cascading Link can be connected to the local Collaboration Server, to an MCU on a higher cascade level or to the Content sharer.
	The first Intra request that is received from any of the Slave MCUs connected to the Collaboration Server starts the interval counter and is forwarded to the next level MCU or to the Content sharer.
	All other Intra requests that are received within this interval are registered but ignored. After an interval of <flag value=""> seconds, the system checks if during the last interval any additional Intra requests were registered. If there is at least one Intra request it will be forwarded. If there is no additional Intra request not no action is taken other than to wait for the next cycle.</flag>
	This filtering process is repeated every <flag value=""> seconds. Default: 30</flag>
CONTENT_SPEAKER_INTRA_S UPPRESSION_IN_SECONDS	This flag controls the requests to refresh (intra) the content sent from the Collaboration Server system to the content sender as a result of refresh requests initiated by other conference participants. Enter the interval in seconds between the Intra requests sent from the
	Collaboration Server to the endpoint sending the content to refresh the content display. Refresh requests that will be received from endpoints within the defined interval will be postponed to the next interval. Default setting: 5

Flag	Description
CPU_TCP_KEEP_ALIVE_TIME_ SECONDS	This flag indicates when to send the first KeepAlive indication to check the TCP connection. Default value: 7200 second (120 minutes) Range: 600-18000 seconds When there are NAT problems, this default may be too long and the TCP connection is lost. In such a case, the default value should be changed to 3600 seconds (60 minutes) or less.
CPU_TCP_KEEP_INTERVAL_SE CONDS	This flag indicates the interval in seconds between the KeepAlive requests. Default value: 75 second Range: 10-720 seconds.
DISABLE_INACTIVE_USER	Users can be automatically disabled by the system when they do not log into the Collaboration Server application for a predefined period. Possible Values: 0 - 90 days. Default: 0 (disables this option). Default (ULTRA_SECURE_MODE=YES): 30
ENABLE_ACCEPTING_ICMP_REDIRECT	When set to YES, allows the RMX to accept ICMP Redirect Messages (ICMP message type #5). For more information see Internet Control Message Protocol (ICMP). Possible values: YES / NO Default: Ultra Secure Mode: NO Standard Security Mode: YES
ENABLE_AGC	Set this flag to YES to enable the AGC option. (Default setting is NO.) When disabled, selecting the AGC option in the <i>Participant Properties</i> has not effect on the participant audio. For more information see Managing the Address Book. The Auto Gain Control mechanism regulates noise and audio volume by keeping the received audio signals of all participants balanced. Note: Enabling AGC may result in amplification of background noise.

Flag	Description
ENABLE_AUTO_EXTENSION	When set to YES , allows conferences running on the Collaboration Server to be automatically extended as long as there are participants connected and the system has free resources.
	Set this flag to NO prevent conference duration from being automatically extended. It can also be used to enable the definition of conference duration that is shorter than is 11 minutes for the RealPresence Collaboration Server (RMX) 1500 and 20 minutes for the RealPresence Collaboration Server (RMX) 2000/4000. Default: YES
	Note: If this flag is set to:
	 YES, Gateway Calls are not limited in duration while endpoints are connected.
	 NO, Gateway Calls are limited to 60 minutes. For more information see Gateway Functionality.
ENABLE_CASCADED_LINK_TO_ JOIN_WITHOUT_PASSWORD	Enables a cascaded link to enter a conference without a password. Default: NO , for security reasons.
ENABLE_CYCLIC_FILE_SYSTE M_ALARMS	Enables or disables the display of Active Alarms before overwriting the older CDR/Auditor/Log files, enabling the users to backup the older files before they are deleted. Default: NO
	Default (ULTRA_SECURE_MODE=YES): YES
ENFORCE_SAFE_UPGRADE	When set to YES this flag enables the Collaboration Server system to notify users when an incorrect version upgrade/downgrade or upgrade/downgrade path is selected.
	When set to NO , after initiating an upgrade or downgrade software installation, the Collaboration Server activates a fault alert in the Faults
	List: Warning: Upgrade started and SAFE Upgrade protection is turned OFF and the upgrade/downgrade process continues.
	Range: YES / NO Default: YES
ENABLE_SENDING_ICMP_DEST INATION_UNREACHABLE	Not supported with RealPresence Collaboration Server (RMX) 1500/1800/2000/4000.
	When set to YES , this flag allows the RMX to send <i>I</i> CMP Destination Unreachable Messages (ICMP message type #3) messages. For more information, see Internet Control Message Protocol (ICMP).
EXT_DB_IVR_PROV_TIME_SEC ONDS	When an Entry Queue is set as IVR Service Provider for the RealPresence DMA system, the value here indicates the time interval in seconds in which the database is accesses for the ID. Default: 300

Flag	Description
FORCE_CIF_PORT_ALLOCATION	Sets the MCU to allocate one CIF video resource to an endpoint, regardless of the resolution determined by the Conference Profile parameters. You can specify the endpoint types for which resource allocation can be forced to CIF resource, enabling other types of endpoints to use higher resolutions in the same conference. Enter the product type to which the CIF resource should be allocated. Possible values are: • CMA Desktop - for CMA desktop client • VSX nnnn - where nnnn represents the model number for example, VSX 8000.
FORCE_STRONG_PASSWORD_ POLICY	When set to YES (default when ULTRA_SECURE_MODE=YES), implements the Strong Password rules. For more details, Changing a User's Password. Default: NO
FORCE_SYSTEM_BROADCAST _VOLUME	If set to YES, the level of broadcasting volume of the connected participant is value taken from the system flag SYSTEM_BROADCAST_VOLUME. If set to NO (default), the broadcasting volume level is 5.
FORCE_SYSTEM_LISTENING_V OLUME	If set to YES, the level of listening volume of the connected participant is value taken from the system flag SYSTEM_LISTENING_VOLUME. If set to NO (default), the listening volume level is 5.
GK_MANDATORY_FOR_CALLS_ IN	If set to YES , a gatekeeper is required to receive incoming H.323 calls. If a gatekeeper is not configure in the Collaboration Server, the calls will fail. If set to NO (default), gatekeeper is not required to process H.323 incoming calls and H.323 participants can dial in with or without a gatekeeper.
GK_MANDATORY_FOR_CALLS_ OUT	If set to YES , a gatekeeper is required to perform H.323 outgoing calls. If a gatekeeper is not configure on the Collaboration Server, the calls will fail. If set to NO (default), gatekeeper is not required to dial out to H.323 participants and calls can be dialed out with or without a gatekeeper.
H263_ANNEX_T	Set to NO to send the content stream without Annex T and enable Aethra and Tandberg endpoints, that do not support Annex T, to process the content. Default: YES
HD_THRESHOLD_BITRATE	Sets the minimum bit rate required by endpoints to connect to an HD Conference. Endpoints that cannot support this bit rate are connected as audio only. Range: 384kbps - 4Mbs (Default: 768)

Flag	Description
HIDE_SITE_NAMES	From version 7.6.1, in MPMx Card Configuration Mode, this flag has been replaced by the Enable Site Names option in the Conference Profile - Site Names dialog box. It allows you to enable or disable the display of site names in conferences per conference. In versions prior to 7.6, set this flag to ON to cancel the display of site names. When set to ON and the display is disabled, the flag SITE_NAMES_ALWAYS_ON =YES is ignored. Default: OFF Note: This option is unavailable in VSW conferences.
INTERNAL_SCHEDULER	When set to NO (default) this flag prevents potential scheduling conflicts from occurring as a result of system calls from external scheduling applications such as Polycom ReadiManager®, CMA™ 4000/5000 and others via the API. Set to YES to schedule conference reservations using an external scheduling application.
ISDN_COUNTRY_ CODE	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The name of the country in which the MCU is located. Default: COUNTRY_NIL
ISDN_IDLE_CODE_E1	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The Idle code (silent), transmitted on the ISDN E1 B channels, when there is no transmission on the channels. Default: 0x54
ISDN_IDLE_CODE_T1	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The Idle code (silent), transmitted on the ISDN T1 B channels, when there is no transmission on the channels. Default: 0x13
ISDN_LEGACY_EP_CLOSE_CO NTENT_FORCE_H263	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. If set to YES , legacy ISDN endpoints that do not support sharing content over the Content channel receive video over video channel that is forced to H.263 video. Default: NO .
ISDN_NUM_OF DIGITS	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. When using ISDN Overlap sending dialing mode, this field holds the number of digits to be received by the MCU. Default: 9

Flag	Description
ISDN_RESOURCE_POLICY (ISDN)	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only.
	The flag value determines how the ISDN B-channels within configured spans are allocated.
	The robustness of the ISDN network can be improved by allocating channels evenly (load balancing) among the spans, minimizing the effect of channel loss resulting from the malfunction of a single span.
	Set the flag value to:
	 LOAD_BALANCE to allocate channels evenly among all configured spans.
	FILL_FROM_FIRST_CONFIGURED_SPAN
	To allocate all channels on the first configured span before allocating channels on other spans.
	FILL_FROM_LAST_CONFIGURED_SPAN
	To allocate all channels on the last configured span before allocating channels on other spans.
	Default: LOAD_BALANCE

Flag Description

ITP_CROPPING

If the conference is set to TelePresence mode, cropping of the image is done according to this flag value:

- ITP (default) Cropping is done as follows:
 - ▲ Left/right sides: no cropping
 - ▲ Top/Bottom: the calculated area to be stripped will be split and cropped equally from the top and the bottom of the display area.



- CP Cropping is done as follows:
 - ▲ Left/right sides: the calculated area to be stripped will be split and cropped equally from the top and bottom of the image
 - ▲ Top/Bottom: the calculated area to be stripped will be split and cropped equally from both sides.



- MIXED Cropping is done as follows:
 - ▲ Left/right sides: the calculated area to be stripped will be split and cropped equally from the top and bottom of the image
 - ▲ Top/Bottom: the calculated area to be stripped will be cropped 84% of the calculated area to be stripped will be cropped from the bottom, and 16%will be cropped from the top.



Note: If the flag was added with no value, and the conference is set to TelePresence mode, cropping is done as follows:

- Left/right sides: no cropping
- Top/Bottom: the calculated area to be stripped will be cropped 84% of the calculated area to be stripped will be cropped from the bottom, and 16%will be cropped from the top.

Flag	Description
IVR_MESSAGE_VOLUME	The volume of IVR messages varies according to the value of this flag. Possible value range: 0-10 (Default: 6). 0 – disables playing the IVR messages 1 – lowest volume 10 – highest volume Notes: It is not recommended to disable IVR messages by setting the flag value to 0. System reset is not required for flag changes to take effect.
IVR_MUSIC_VOLUME	The volume of the IVR music played when a single participant is connected to the conference varies according to the value of this flag. Possible value range: 0-10 (Default: 5). 0 – disables playing the music 1 – lowest volume 10 – highest volume Note: System reset is not required for flag changes to take effect.
IVR_ROLL_CALL_USE_TONES_I NSTEAD_OF_VOICE	This flag is applicable in versions prior to version 7.6. In version 7.6 this flag is replaced by IVR Service - Roll Call/Notifications options. When set to YES , the system does not playback the Roll Call names when participants enter or exit the conference. If the voice messages are replaced with tones the system will play these tones instead. The use of tones requires the uploading of the appropriate tone files in *wav format and replacing the Roll Call Joined and Roll Call Left message files with the tone files in the Conference IVR Service - Roll Call dialog box. When the flag is set to NO, Roll Call names are announced when participants enter or exit the conference. Default: NO.
IVR_ROLL_CALL_VOLUME	The volume of the Roll Call varies according to the value of this flag. Possible value range: 0-10 (Default: 6). 0 – disables playing the Roll Call 1 – lowest volume 10 – highest volume Note: It is not recommended to disable the Roll Call by setting the flag value to 0. System reset is not required for flag changes to take effect.
LAST_LOGIN_ATTEMPTS	If YES , the system displays a record of the last Login of the user. Default: NO . For more details, see User Login Record.

Flag	Description
LEGACY_EP_CONTENT_DEFAU LT_LAYOUT	Defines the video layout to be displayed on the screen of the legacy endpoints when switching to Content mode. Default value: CP_LAYOUT_1P7 (1+7). For a detailed list of possible flag values for the various video layouts, see Legacy Endpoint Content Default Layout Flag Values.
MAX_CONF_PASSWORD_REPE ATED_CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters that are to be allowed in a conference password. Range: 1 - 4 Default: 2 Note: In Version 7.7, if a Polycom DMA system is installed in your environment, you must change the value of this flag to 4 to maintain the compatibility between the Collaboration Server and the DMA.
MAX_CP_RESOLUTION	The MAX_CP_RESOLUTION flag value is applied to the system during First Time Power-on and after a system upgrade. The default value is HD1080. All subsequent changes to the Maximum CP Resolution of the system are made using the Resolution Configuration dialog box. Possible flag values: • HD1080 – High Definition at 60 fps • HD1080 – High Definition at 30 fps • HD720 – High Definition at 30 fps • HD – High Definition at 30 fps • SD30 – Standard Definition at 30 fps • SD15 – Standard Definition at 15 fps • CIF – CIF resolution Default: HD1080 For more information see Video Resolutions in AVC-based CP Conferencing.
MAX_INTRA_REQUESTS_PER_I NTERVAL_	Enter the maximum number of refresh (intra) requests for the Content channel sent by the participant's endpoint in a 10 seconds interval that will be dealt by the Collaboration Server system. When this number is exceeded, the Content sent by this participant will be identified as noisy and his/her requests to refresh the Content display will be suspended. Default setting: 3
MAX_INTRA_SUPPRESSION_D URATION_IN_SECONDS_	Enter the duration in seconds to ignore the participant's requests to refresh the Content display. Default setting: 10
MAX_NUMBER_OF_MANAGEM ENT_SESSIONS_PER_SYSTEM	Defines the maximum number of concurrent management sessions (http and https connections) per system. Value: 4 - 80 Default: 80

Flag	Description
MAX_NUMBER_OF_MANAGEM ENT_SESSIONS_PER_USER	Defines the maximum number of concurrent management sessions (http and https connections) per user. Value: 4 - 80 Default: 10 (20 in Ultra Secure Mode)
MAX_PASSWORD_REPEAPED_ CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a user password. Range: 1 - 4 Default: 2
MAX_PASSWORD_REPEATED_ CHAR	Allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a password. Range: 1 - 4 Default: 2
MCU_DISPLAY_NAME	The name of the MCU that is displayed on the endpoint's screen when connecting to the conference. Default: POLYCOM RMX 1500/POLYCOM RMX 2000/ POLYCOM RMX 4000POLYCOM RealPresence Collaboration Server 1800depending on the product type.
MIN_PASSWORD_LENGTH	The length of passwords. Possible value: between 0 and 20. 0 means this rule is not enforced, however this rule cannot be disabled when the Collaboration Server is in Ultra Secure Mode. In Ultra Secure Mode, passwords must be at least 15 characters in length (default) and can be up to 20 characters in length. For more details, see Password Length.
MIN_PWD_CHANGE_FREQUEN CY_IN_DAYS	Defines the frequency with which a user can change a password. Values: 0 -7. 0 (standard default) - users do not have to change their passwords. In Ultra Secure Mode the retention period is between 1 (default) and 7. For details, see Defining Password Change Frequency.
MIN_SYSTEM_DISK_SPACE_TO _ALERT	Defines a minimum remaining Collaboration Server disk capacity in megabytes. If the remaining disk capacity falls below this level an active alarm is raised. Default: 2048
MIN_TIP_COMPATIBILITY_LINE_ RATE	This flag determines the minimum line rate at which conferencing entities such as an Entry Queue or Meeting Room can be TIP-enabled and TIP-enabled endpoints can connect to them. CTS version 7 requires a minimum line rate of 1024 kbps and will reject calls at lower line rates, therefore the System Flag value should be 1024 kbps or higher. O means that no minimum line rate is enforced on the conference for TIP connectivity. Default: 1024

Flag	Description
MS_ENVIRONMENT	If YES , sets the Collaboration Server SIP environment to integrate with Microsoft OCS solution. Default: NO
MULTIPLE_SERVICES	Determines whether the Multiple Services option is be activated once the appropriate license is installed. Possible Values: YES / NO Default: NO Note: If the MULTIPLE_SERVICES System Flag is set to YES and no RTM ISDN or RTM LAN card is installed in the RealPresence Collaboration Server (RMX) 2000, an Active Alarm is displayed.
NUM_OF_LOWER_CASE_ALPH ABETIC	The minimum number of lower case alphabetic characters required in a Login password in Ultra Secure Mode. Default: 0
NUM_OF_NUMERIC	The minimum number of numeric characters required in a Login password in Ultra Secure Mode. Default: 0
NUM_OF_SPECIAL_CHAR	The minimum number of special characters (asterisks, brackets, periods etc.) required in a Login password in Ultra Secure Mode. Default: 0
NUM_OF_UPPER_CASE_ALPHA BETIC	The minimum number of upper case alphabetic characters required in a Login password in Ultra Secure Mode. Default: 0
NUMERIC_CHAIR_PASS_DEFA ULT_LEN	 This flag enables or disables the automatic generation of chairperson passwords and determines the number of digits in the chairperson passwords assigned by the MCU. Possible values are: • 0 disables the automatic password generation in both Standard Security Mode or Ultra Secure Mode. Any value other than 0 enables the automatic generation of chairperson passwords if the flag HIDE_CONFERENCE_PASSWORD is set to NO. • 1 – 16, default: 6 (Standard Security Mode) • 9 – 16, default: 9 (Ultra Secure Mode). If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.
NUMERIC_CHAIR_PASS_MAX_L EN	The maximum number of digits that the user can enter when manually assigning a password to the chairperson. Range: • 0 – 16 (Standard Security Mode) • 9 – 16 (Ultra Secure Mode). Default (both Modes): 16

Flag	Description
NUMERIC_CHAIR_PASS_MIN_L EN	Defines the minimum length required for the Chairperson password. Value: 0-16 Default: 0 - (Standard Security Mode) this rule is not enforced. However this rules cannot be disabled when the Collaboration Server is in Ultra Secure Mode. 9 - (Ultra Secure Mode) Chairperson password must be at least 9 characters in length (default).
NUMERIC_CONF_ID_LEN	Defines the number of digits in the Conference ID that will be assigned by the MCU. Enter 0 to disable the automatic assignment of IDs by the MCU and let the Collaboration Server user manually assign them. Range: 2-16 (Default: 4).
NUMERIC_CONF_ID_MAX_LEN	The maximum number of digits that the user can enter when manually assigning an ID to a conference. Range: 2-16 (Default: 8) Note: Selecting 2 limits the number of simultaneous ongoing conferences to 99.
NUMERIC_CONF_ID_MIN_LEN	The minimum number of digits that the user must enter when manually assigning an ID to a conference. Range: 2-16 (Default: 4) Note: Selecting 2 limits the number of simultaneous ongoing conferences to 99.
NUMERIC_CONF_PASS_DEFAU LT_LEN	 This flag enables or disables the automatic generation of conference passwords and determines the number of digits in the conference passwords assigned by the MCU. Possible values are: O disables the automatic password generation in both Standard Security Mode or Ultra Secure Mode. Any value other than 0 enables the automatic generation of conference passwords if the flag HIDE_CONFERENCE_PASSWORD is set to NO. 1 – 16, default: 6 (Standard Security Mode) 9 – 16, default: 9 (Ultra Secure Mode). If the default is used, in non-secured mode the system will automatically generate conference passwords that contain 6 characters.
NUMERIC_CONF_PASS_MAX_L EN	The maximum number of digits that the user can enter when manually assigning a password to the conference. Range: • 0 – 16 (Standard Security Mode) • 9 – 16 (Ultra Secure Mode). Default (both Modes): 16

Flag	Description
NUMERIC_CONF_PASS_MIN_L EN	Defines the minimum length required for the Conference password. Value: 0-16 Default:
	 0 - (Standard Security Mode) this rule is not enforced. However this rules cannot be disabled when the Collaboration Server is in Ultra Secure Mode.
	9 - (Ultra Secure Mode) Conference password must be at least 9 characters in length (default).
PAL_NTSC_VIDEO_OUTPUT	When set to AUTO (default), the video output sent by the Collaboration Server is either PAL or NTSC format, depending on the current speaker in the layout. This ensures full synchronization between the frame rate of the speaker and the video encoder, ensuring smoother video.
	In environments where the majority of endpoints are configured to either NTSC or PAL, the flag can be set accordingly to change the video encoding of the Collaboration Server to be compatible with the majority of endpoints in the call. Possible Values: AUTO , PAL , NTSC
PASSWORD_EXPIRATION_DAY	Determines the duration of password validity.
s	Value: between 0 and 90 days.
	0 - user passwords do not expire. In <i>Ultra Secure Mode</i> : default - 60 days, the minimum duration is 7 days.
	For details, see Defining Password Aging.
PASSWORD_EXPIRATION_DAY S_MACHINE	Enables the administrator to change the password expiration period of <i>Application-user</i> 's independently of regular users. Default: 365 (days).
PASSWORD_EXPIRATION _WARNING_DAYS	Determines the display of a warning to the user of the number of days until password expiration.
	Value: between 0 and 14 days. 0 - password expiry warnings are not displayed. In <i>Ultra Secure Mode</i> ,
	the earliest display - 14 days, the latest 7 days (default).
	For details, see Defining Password Aging.
PASSWORD_HISTORY_SIZE	The number of passwords that are recorded to prevent users from re-using their previous passwords.
	Values are between 0 and 16.
	0 (standard default) - the rule is not enforced, however this rule cannot be disabled when the Collaboration Server is in Ultra Secure Mode.In <i>Ultra Secure Mode</i> , at least 10 passwords (default) and up to 16 passwords must be retained.
	For more details, see Implementing Password Re-Use / History Rules.
RESTRICT_CONTENT_BROADC AST_TO_LECTURER	If set to YES , only the conference lecturer may send content to the conference. If set to NO , any conference participant can send content.
	Default: YES

Flag	Description
RMX2000_RTM_LAN	This flag is used after installation on and RTM-LAN card to activate the card. The flag must be set to YES . (RealPresence Collaboration Server (RMX) 2000 only.)
RRQ_WITHOUT_GRQ	To enable registration, some gatekeepers require sending first RRQ and not GRQ. Set flag to YES , if this behavior is required by the gatekeeper in your environment. Default: NO . GRQ (Gatekeeper Request) - Gatekeeper discovery is the process an endpoint uses to determine which gatekeeper to register with. RRQ - registration request sent to the gatekeeper.
SEPARATE_MANAGEMENT_NE TWORK	Enables/disables the Network Separation. Can only be disabled in the Ultra Secure Mode (ULTRA_SECURE_MODE= YES). Default: NO .
SESSION_TIMEOUT_IN_MINUT ES	If there is no input from the user or if the connection is idle for longer than the number of minutes specified by this flag, the connection to the Collaboration Server is terminated. Value: 0-999 0 - Session Timeout is disabled, however this feature cannot be disabled when the Collaboration Server is in Ultra Secure Mode. Default: 0 Default (ULTRA_SECURE_MODE=YES): 10
SIP_AUTO_SUFFIX_EXTENSIO N	Used to automatically add a suffix to a SIP address (To Address) instead of adding it manually in the Collaboration Server Web Client (SIP address) when the SIP call is direct-dial and not through a Proxy. Example: Participant Name = john.smith Company Domain = maincorp.com SIP_AUTO_SUFFIX_EXTENSION flag value = @maincorp.com Entering john.smith will generate a SIP URI = john.smith@maincorp.com
SITE_NAMES_LOCATION	This flag is not supported from version 8.1. This function is controlled using the Profile -Site Names dialog box.
STAR_DELIMITER_ALLOWED	When set to YES , an asterisk "*" can be used as a delimiter in Conference and Meeting Room dial strings. The dial string is first searched for "'#" first followed by "*". Default: NO

Flag	Description
SYSTEM_BROADCAST_VOLUM E	This value is used when the system flag FORCE_SYSTEM_BROADCAST_VOLUME is set to YES. Determines the default audio level with which the participants connects and sends audio to the conference. The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default connection value is 5. Each unit change represents an increase or decrease of 3 dB (decibel). Range: 1-10 Default: 5
SYSTEM_LISTENING_VOLUME	This value is used when the system flag FORCE_SYSTEM_LISTENING_VOLUME is set to YES. Determines the default audio level with which the participants connects and receives audio from the conference. The volume scale is from 1 to 10, where 1 is the weakest and 10 is the strongest. The default value is 5. Each unit change represents an increase or decrease of 3 dB (decibel). Range: 1-10 Default: 5
TERMINATE_CONF_AFTER_CH AIR_DROPPED	From Version 8.1, this flag's functionality is replaced by the Terminate Conference after Chairperson Drops check box in the Profile - IVR dialog box. In versions prior to 8.1, if YES, sets conferences to automatically terminate if the Chairperson disconnects from the conference. This takes effect only if the Conference Requires Chairperson check box in the Conference Profile Properties, IVR Tab, is selected. Default: YES Note: In order for the "Chairperson Exit" message to be played this flag must be set to YES.
ULTRA_SECURE_MODE	When set to YES enables the Ultra Secure Mode. When enabled, affects the ranges and defaults of the System Flags that control: Network Security User Management Strong Passwords Login and Session Management Cyclic File Systems alarms Default: NO For a list of flags affected when the Ultra Secure Mode is enabled, see System Flags affected by Ultra Secure Mode.

Flag	Description
USE_GK_PREFIX_FOR_PSTN_ CALLS	When set to YES the <i>Gatekeeper Prefix</i> is included in the <i>DTMF</i> input string enabling <i>PSTN</i> participants to use the same input string when connecting to an Collaboration Server whether the Collaboration Server is a standalone MCU or part of a <i>DMA</i> solution deployment. Possible Values: YES / NO Default: NO For more information see PSTN Dial-in Using GK Prefix.
USER_LOCKOUT	If YES, a user is locked out of the system after three consecutive Login failures with same User Name. The user is disabled and only the administrator can enable the user within the system. Default: NODefault in Ultra Secure Mode: YES For details, see User Lockout
USER_LOCKOUT_DURATION_I N_MINUTES	Defines the duration of the Lockout of the user. Value: 0 - 480 0 means permanent User Lockout until the administrator re-enables the user within the system. Default: 0
USER_LOCKOUT_WINDOW_IN_ MINUTES	Defines the time period during which the three consecutive Login failures occur. Value: 0 - 45000 0 means that three consecutive Login failures in any time period will result in User Lockout. Default: 60

Manually Adding and Deleting System Flags

To add a flag:

1 In the System Flags dialog box, click the New Flag button.
The New Flag dialog box is displayed.



- 2 In the **New Flag** field enter the flag name.
- 3 In the Value field enter the flag value.

The flags in the **Manually Added, Modified, Deleted System Flags** table can be manually added to the **MCMS_PARAMETERS_USERS** tab.

4 Click **OK** to close the **New Flag** dialog box.

The new flag is added to the flags list.

5 Click **OK** to close the **System Flags** dialog box.



For flag changes (including deletion) to take effect, reset the MCU.

Manually Added, Modified, Deleted System Flags

Flag	Description
802_1X_CERTIFICATE_MODE	Not supported with RealPresence Collaboration Server (RMX) 1500/1800/2000/4000.
	Determines whether one TLS certificate is retrieved from the Certificate Repository for all IP services or if multiple certificates will be retrieved, one for each IP service. For more information, see IEEE 802.1X Authentication.
	Range: ONE_CERTIFICATE, MULTIPLE_CERTIFICATE
	Default: ONE_CERTIFICATE. Note: Not Supported in RMX 1800.
802_1X_SKIP_CERTIFICATE_VA LIDATION	Not supported with RealPresence Collaboration Server (RMX) 1500/1800/2000/4000. If the flag value is: • YES - The retrieved certificate is not validated against the CA certificate. • NO - The retrieved certificate is validated against the CA certificate. Validation failure raises an Active Alarm and is reported in the Ethernet Monitoring dialog box. For more information, see IEEE 802.1X Authentication. Range: YES, NO Default: YES
802_FIPS_MODE	Not supported with RealPresence Collaboration Server (RMX) 1500/1800/2000/4000. If the flag value is YES , the availability of the MD5 Authentication Protocol will neither be displayed as selectable option nor supported. For more information, see IEEE 802.1X Authentication. Range: YES/NO . Default: NO

Flag	Description
ACCEPT_VOIP_DTMF_TYPE	Defines the type of DTMF tones (inband) or digits (outband) that the Collaboration Server will accept in VOIP calls. Range: O - Auto (default): Inband or outband DTMF tones/digits are accepted depending on the endpoint's current setting. If the endpoint switches from inband to outband or visa versa the value of the SET_DTMF_SOURCE_DIFF_IN_SEC flag determines the time interval after which both inband and outband tones/digits will be accepted. 1 - Outband (H.245) only 1 - Inband only
ALLOW_NON_ENCRYPT_PART Y_IN_ENCRYPT_CONF	If YES, allows non-encrypted participants to connect to encrypted conferences. Default: No Note: From Version 7.6.1, this flag is replaced by the Encryption option "Encrypt when Possible" in the conference Profile - Advanced dialog box. Flag setting is ignored.
ALWAYS_FORWARD_DTMF_IN_ GW_SESSION_TO_ISDN (ISDN)	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. When set to YES, all DTMF codes sent by participants in the GW session will be forwarded to all PSTN and ISDN participants in the same GW session. Range: YES / NO Default Value: NO
ANAT_IP_PROTOCOL	If YES, enables Alternative Network Address Types. For more information, see Alternative Network Address Types (ANAT). Range: DISABLED, AUTO, PREFER_IPv4, PREFER_IPv6 Default: ULTRA SECURE MODE: NO STANDARD SECURITY MODE: YES
APACHE_KEEP_ALIVE_TIMEOU T	If the connection is idle for longer than the number of seconds specified by this flag, the connection to the Collaboration Server is terminated. Value: 0 - 999 Default: 15 Default (ULTRA_SECURE_MODE=YES): 15 Note: A value of 0 results in an unlimited keep-alive duration. This value should never be used in <i>Ultra Secure Mode</i> .
AVOID_VIDEO_LOOP_BACK_IN _CASCADE	When set to YES the current speaker's image is not sent back through the participant link in cascaded conferences with conference layouts other than 1x1. Default: YES Range: YES / NO

Flag	Description
BLOCK_CONTENT_LEGACY_F OR_LYNC	This flag is used to control the system behavior in an environment where some Lync clients use the Polycom CCS plug-in and some do not. When set to NO (default), Content is sent to all Lync clients over the video channel, including those with the plug-in installed, even when the Send Content to Legacy Endpoints is disabled. Other, non-Lync legacy endpoints will not be affected by this flag and will receive content according to the Send Content to Legacy Endpoints settings in the conference Profile. When set to YES , Content is not sent to Lync clients over the video channel including those with the Polycom CCS plug-in installed, even when the Send Content to Legacy Endpoints is enabled. Other, non-Lync legacy endpoints will not be affected by this flag and will receive content according to the Send Content to Legacy Endpoints settings in the conference Profile.
BONDING_DIALING_METHOD (ISDN)	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. When set to: SEQUENTIAL The MCU initiates channel connections sequentially until it reaches the number of channels defined by the BONDING_NUM_CHANNELS_IN _GROUP flag. When a channel is connected, dialing begins for the next channel in the group. BY_TIMERS The MCU initiates channel connections sequentially using the values of the BONDING_CHANNEL_DELAY and BONDING_GROUP_DELAY flags. The first group of channels is dialed, using the BONDING_CHANNEL_DELAY between dialing attempts for each channel in the group. The Collaboration Server then implements the BONDING_GROUP_DELAY, before dialing the first channel of the next group. Default: SEQUENTIAL
BONDING_GROUP_DELAY (ISDN)	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. When connecting several bonding groups, this is the delay (number of 1/100 seconds) preceding the first dialing attempt to connect the next bonding group. Default: 500

Flag	Description
BONDING_NUM_CHANNELS_IN _GROUP (ISDN)	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The number of channels in the bonding group to be connected before dialing the next sequential channel. Default: 50
BURN_BIOS	Although <u>not recommended</u> , setting this flag's value to NO will prevent BIOS upgrade. Default: YES.
CAC_ENABLE	When set to YES, enables the Call Admission Control implementation in the Collaboration Server. Default: NO (CAC is disabled)
CASCADE_LINK_PLAY_TONE_ ON_CONNECTION	When set to YES , the RealPresence Collaboration Server plays a tone when a cascading link between conferences is established. The tone is played in both conferences. This tone is not played when the cascading link disconnects from the
	conferences. The tone used to notify that the cascading link connection has been established cannot be customized. Default value: NO. The tone volume is controlled by the same flag as the IVR messages and tones: IVR_MESSAGE_VOLUME.
CELL_IND_LOCATION	Change the location of the display of Network Quality Indicators displayed in the cells of the conference Video Layout. Default: TOP_RIGHT Range: BOTTOM_LEFT BOTTOM_RIGHT TOP_LEFT TOP_RIGHT
CFG_KEY_ENABLE_FLOW_CO NTROL_REINVITE	Used to enable or disable sending a <i>re-INVITE</i> to endpoints to adjust their data rate. When set to YES, <i>re-INVITE</i> is used for endpoints that do not support <i>flow control</i> in SIP using either the <i>Information</i> or <i>RTCP Feedback</i> mechanisms. Default: NO.
CONF_GATHERING_DURATION _SECONDS	The value of this <i>System Flag</i> sets the duration of the <i>Gathering Phase</i> in seconds. The <i>Gathering Phase</i> duration of the conference is measured from the scheduled start time of the conference. Range: 0 - 3600 Default: 180 For more information see Video Preview (AVC Participants Only)

Flag	Description
CP_REGARD_TO_INCOMING_S ETUP_RATE	For use in the Avaya Environment. If set to YES, the RealPresence Collaboration Server calculates the line rate for incoming calls in CP conferences, according to the line rate which is declared by the endpoint in the H.225 setup message. If set to NO, the rate is calculated according to the conference line rate regardless of the rate in the H.225 setup message. Default: YES.
CPU_BONDING_LINK_MONITO RING_FREQUENCY	Used when using the <i>MII Monitor</i> for troubleshooting networks. This flag sets the <i>MII Polling Interval</i> in milliseconds. A value of zero disables <i>MII</i> monitoring. Default: 100
CPU_BONDING_MODE	Sets the Bonding Mode of the Signalling and Management network interface controllers. Mode=6, balance-alb, (Adaptive Load Balancing) includes balance-tlb, (Transmit Load Balancing) and balance-rlb (Receive Load Balancing) for IPV4 traffic. No special switch support is required. Receive Load Balancing is achieved by ARP negotiation. Outbound ARP Replies are intercepted and their source hardware address is overwritten with the unique hardware address of one of the slaves in the bond. In this way different peers will use different hardware addresses for the server. Note: balance-alb is the only supported value. All other possible values are for troubleshooting purposes only. Default: balance-alb Possible values: balance-alb balance-rr active-backup balance-xor broadcast 802.3ad balance-tlb
DETECT_SIP_EP_DISCONNEC T_TIMER	The flag value indicates the amount of time in seconds to wait for an RTCP or RTP message to be received from the endpoint. When the time that was set in the system flag has elapsed and no RTCP or RTP audio or video message has been received on either the audio or the video channel, the MCU disconnects the SIP endpoint from the conference. Default: 20 (seconds) Range: 0 - 300 For more information see Detecting SIP Endpoint Disconnection.

Flag	Description
DELAY_BETWEEN_H320_DIAL_ OUT_PARTY (ISDN)	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The delay in milliseconds that the MCU waits when connecting dial out ISDN and PSTN participants. Default: 1000
DISABLE_CELLS_NETWORK_IN D	Disable the display of <i>Network Quality Indicators</i> displayed in the cells of the conference <i>Video Layout</i> . Default: YES Range: YES / NO
DISABLE_DUMMY_REGISTRATI ON	Enables or disables SIP dummy registration on the domain. Possible Values: NO (Default) - Disables SIP dummy registration. YES - Enables SIP dummy registration. Note: For homologation and certification testing, the flag must be set to YES.
DISABLE_GW_OVERLAY_INDIC ATION	When set to NO (default), displays progress indication during the connection phase of a gateway call. Set the value to YES to hide the connection indications displayed on the participant's screen during the connection phase of a gateway call.
DISABLE_SELF_NETWORK_IN D	Disable the display of the <i>Network Quality Indicator</i> of the participant's own endpoint. Default: NO Range: YES / NO
DISABLE_WIDE_RES_TO_SIP_ DIAL_OUT	When set to NO (default), the RealPresence Collaboration Server sends wide screen resolution to dial-out SIP endpoints. Endpoint types that do not support wide screen resolutions are automatically identified by the Collaboration Server according to their product type and version and will not receive the wide resolution even if the flag is set to YES. When manually added and set to YES , the RealPresence Collaboration Server does not send wide screen. Default: NO.
DTMF_FORWARD_ANY_DIGIT_ TIMER_SECONDS	Used for DTMF code suppression in cascading conferences. Determines the time period (in seconds) that MCU A will forward DTMF inputs from conference A participants to MCU B. Flag range (in seconds): 0 - 360000 This flag is defined on MCU A (the calling MCU). For more information, see Setting the Video Layout in Cascading conferences (CP and mixed CP and SVC).
ENABLE_1080_SVC	When set to YES <i>HD1080p30</i> is enabled as the highest supported resolution in <i>SVC</i> mode. Range: YES / NO Default: NO

Flag	Description
ENABLE_CISCO_GK	When set to YES, it enables the use of an identical prefix for different Collaboration Servers when registering with a Cisco MCM Gatekeeper. Default: NO.
ENABLE_CLOSED_CAPTION	Enables or disables the Closed Captions option that allow endpoints to endpoints to provide real-time text transcriptions or language translations of the video conference. When set to NO (default), Closed Captions are disabled. When set to YES, Closed Captions are enabled.
ENABLE_EPC	When set to YES (default), enables Polycom proprietary People+. When set to NO, disables this feature for all conferences and participants.
ENABLE_FLOW_CONTROL_REI NVITE	Used to enable or disable sending a <i>re-INVITE</i> to endpoints to adjust their data rate. When set to YES, <i>re-INVITE</i> is used for endpoints that do not support <i>flow control</i> in SIP using either the <i>Information</i> or <i>RTCP Feedback</i> mechanisms. Default: NO.
ENABLE_EXTERNAL_DB_ACCE SS	If YES, the Collaboration Server connects to an external database application, to validate the participant's right to start a new conference or access a conference. Default: NO
ENABLE_H239	When set to YES, Content is sent via a separate Content channel. Endpoints that do not support H.239 Content sharing will not be able to receive When set to NO, the Content channel is closed. In such a case, H.239 Content is sent via the video channel ("people" video) enabling endpoints that do not support H.239 Content sharing to receive the Content in their video channel. Default: YES.
ENABLE_H239_ANNEX_T	In H.239-enabled MIH Cascading, when MGC is on level 1, enables sending Content using Annex T.
ENABLE_IP_REDIAL	In all versions up to version 7.0, when set to YES (default), it enables re-dialing if H.323 or SIP dial out calls fail. In version 7.0 and later, this flag functionality is replaced by the Auto Redialing check box in the <i>Profile Properties - Advanced</i> dialog box
ENABLE_LYNC_RTCP_INTRA	When set to YES, RTCP FIR is used for sending Intra Requests. When set to NO Intra Requests are sent using SIP INFO Messages. Range: YES / NO Default: NO

Flag	Description
ENABLE_MCCF	Enables or disables the support of External IVR Services via the MCCF-IVR package is enabled. In Ultra Secure Mode and in secured environments where the External IVR Services via the MCCF-IVR package is not required and unused ports should be closed, this flag should be set to NO. Range: YES / NO Default: YES (in Standard security Mode) or NO (in Ultra Secure Mode)
ENABLE_MS_FEC	Enables the Microsoft FEC (Forward Error Correction) support for RTV. Range: Auto/No Default: Auto When set to Auto , FEC support is enabled. FEC uses the DV00 option (DV=00 - one FEC per frame using XOR). When set to No , FEC support is disabled.
ENABLE_NO_VIDEO_RESOUR CES_AUDIO_ONLY_MESSAGE	Enables playing a voice message that Informs the participant of the lack of Video Resources in the RealPresence Collaboration Server and that he/she is being connected as Audio Only. Default: YES
ENABLE_SELECTIVE_MIXING	Enables (default) or disables the Automatic muting of noisy AVC endpoints. For more details, see Automatic Muting of Noisy Endpoints (AVC Endpoints). When set to YES, the automatic muting of noisy endpoints can be enabled or disabled at the conference level in the Conference Profile - Audio Settings dialog box. When set to NO, the automatic muting of noisy endpoints is disabled at the conference level and cannot be enabled in the Conference Profile - Audio Settings dialog box. Default: YES Note: MCU reset is not required when changing the flag value.
ENABLE_SIP_PEOPLE_PLUS_C ONTENT	If security is of higher priority than SIP Content sharing, SIP People+Content can be disabled by setting this System Flag to NO. (The content management control (BFCP) utilizes an unsecured channel (60002/TCP) even when SIP TLS is enabled.) Default: YES
ENABLE_SIP_PPC_FOR_ALL_U SER_AGENT	When set to YES, SIP People+Content and BFCP capabilities are declared with all vendors' endpoints. Default: YES Range: YES / NO
ENABLE_SIRENLPR	Enable / disable SirenLPR Audio Algorithm for use in IP (H.323, SIP) calls in both CP and VSW conferences. Range: YES / NO Default: YES

Flag	Description
ENABLE_SIRENLPR_SIP_ENCR YPTION	Enables the <i>SirenLPR</i> audio algorithm when using encryption with the <i>SIP</i> protocol. Range: YES / NO Default: NO
ENABLE_TC_PACKAGE	Enables or disables Network Traffic Control. Range: YES / NO Default: NO
ENABLE_TEXTUAL_CONFEREN CE_STATUS	Set the value of this flag to NO to disable <i>Text Indication</i> . This setting is recommended for MCUs running Telepresence conferences. Default: YES.
ENABLE_VIDEO_PREVIEW	Enables the Video Preview feature. Default: YES. For more details, see Video Preview (AVC Participants Only).
EXTERNAL_CONTENT_ DIRECTORY	The Web Server folder name. Change this name if you have changed the default names used by the CMA/XMA application. Default: /PlcmWebServices
EXTERNAL_CONTENT_IP	Version 4.x and earlier - enter the IP address of the CMA server. Version 5.0 - enter the IP address of the CMA/XMA server in the format: http://[IP address of the CMA server]. For example, http://172.22.185.89. This flag is also the trigger for replacing the internal Collaboration Server address book with the CMA global Address Book. When empty, the integration of the CMA address book with the Collaboration Server is disabled.
EXTERNAL_CONTENT_PASSW ORD	The password associated with the user name defined for the Collaboration Server in the CMA/XMA server.
EXTERNAL_CONTENT_PORT	The CMA/XMA port used by the Collaboration Server to send and receive XML requests/responses. Default: 80.
EXTERNAL_CONTENT_USER	The login name defined for the Collaboration Server in the CMA/XMA server defined in the format: domain name/user name.
EXTERNAL_DB_DIRECTORY	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The URL of the external database application. For the sample script application, the URL is: <virtual directory="">/SubmitQuery.asp</virtual>

Flag	Description
EXTERNAL_DB_IP	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The IP address of the external database server, if one is used. Default: 0.0.0.0
EXTERNAL_DB_LOGIN	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The login name defined for the Collaboration Server in the external database server. Default: POLYCOM
EXTERNAL_DB_PASSWORD	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The password associated with the user name defined for the Collaboration Server on the external database server. Default: POLYCOM
EXTERNAL_DB_PORT	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. The external database server port used by the Collaboration Server to send and receive XML requests/responses. For secure communications set the value to 443. Default: 5005.
FADE_IN_FADE_OUT	Not supported from version 8.1
FORCE_1X1_LAYOUT_ON_CAS CADED_LINK_CONNECTION	When set to YES , the cascaded link is automatically set to Full Screen (1x1) in CP conferences forcing the speaker in one cascaded conference to display in full window in the video layout of the other conference. Set this flag to NO when connecting to an MGC using a cascaded link, if the MGC is functioning as a Gateway and participant layouts on the other network are not to be forced to 1X1. Default: YES

Flag	Description
FORCE_AUDIO_CODEC_FOR_ MS_SINGLE_CORE	 This flag is used to force the use of a specific Audio algorithm when a Microsoft Office Communicator R2 or Lync Client is hosted on a workstation with a single core processor. The flag value overrides the default audio algorithm selection (G.722.1) that may cause audio quality problems when G.722.1 is used by Microsoft Clients running on single processor workstations. This flag can be set to: AUTO – No forcing occurs and the Collaboration Server negotiates a full set of Audio algorithm during capabilities exchange. G711A/U or G722 – Set this flag value according to the hosting workstation capabilities. If the Collaboration Server detects single core host during capabilities exchange it will assign a G.711 or G.722 Audio algorithm according to the flag value. Possible values: AUTO, G711A, G711U, G722 Default: G711A
FORCE_ENCRYPTION_FOR_U NDEFINED_PARTICIPANT_IN_W HEN_AVAILABLE_MODE	When set to YES , <i>Undefined participants</i> must connect encrypted, otherwise they are disconnected. When set to NO (default) and the conference <i>Encryption</i> in the <i>Profile</i> is set to "Encrypt When Possible", both Encrypted and Non-encrypted <i>Undefined participants</i> can connect to the same conferences, where encryption is the preferred setting. Default: NO
FORCE_G711A	Setting this flag forces the use of the <i>G711A Audio Codec</i> . Possible values: YES / NO Default: NO
FORCE_RESOLUTION	Use this flag to specify IP (H.323 and SIP) endpoint types that cannot receive wide screen resolution and that were not automatically identified as such by the Collaboration Server. Possible values are endpoint types, each type followed by a semicolon. For example, when disabling Wide screen resolution in an HDX endpoint enter the following string: HDX; Note: Use this flag when the flag SEND_WIDE_RES_TO_IP is set to YES.
FORCE_STATIC_MB_ENCODIN G	This flag supports Tandberg MXP mode of sending and receiving video by IP endpoint in HD 720p resolution and Video Quality set to Motion. This mode is not supported for ISDN endpoints. Default value: Tandberg MXP . To disable this flag, enter NONE .
G728_IP	Enables or disables declaration of G.728 Audio Algorithm capabilities in IP calls. Range: YES / NO Default: NO

Flag	Description
G728_ISDN	Applicable to the RealPresence Collaboration Server (RMX) 1500/2000/4000 only. Enables or disables declaration of G.728 Audio Algorithm capabilities in ISDN calls. Range: YES / NO Default: NO
H239_FORCE_CAPABILITIES	When the flag is set to NO, the Collaboration Server only verifies that the endpoint supports the Content protocols: Up to H.264 or H.263. When set to YES, the Collaboration Server checks frame rate, resolution and all other parameters of the Content mode as declared by an endpoint before receiving or transmitting Content. Default: NO.
H264_BASE_PROFILE_MIN_RA TE_CIF60_MOTION	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for CIF60 resolution using Motion Video Quality. Default: 256kbps
H264_BASE_PROFILE_MIN_RA TE_HD1080P30_SHARPNESS	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for HD1080P30 resolution using Sharpness Video Quality. Default: 1536kbps
H264_BASE_PROFILE_MIN_RA TE_HD720P30_SHARPNESS	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for HD720P30 resolution using Sharpness Video Quality. Default: 1024kbps
H264_BASE_PROFILE_MIN_RA TE_HD720P60_MOTION	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for HD720P60 resolution using Motion Video Quality. Default: 1536kbps
H264_BASE_PROFILE_MIN_RA TE_SD30_SHARPNESS	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for SD30 resolution using Sharpness Video Quality. Default: 256kbps
H264_BASE_PROFILE_MIN_RA TE_SD60_MOTION	Not supported from Version 7.0.2. Prior to Version 7.0.2, this flag set the minimum bitrate threshold for endpoints that did not support H.264 High Profile for SD60 resolution using Motion Video Quality. Default: 1024kbps

Flag	Description
H264_HD_GRAPHICS_MIN_CO NTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Graphics. Range: 0-1536 Default: 128
H264_HD_HIGHRES_MIN_CON TENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Hi Resolution Graphics. Range: 0-1536 Default: 256
H264_HD_LIVEVIDEO_MIN_CO NTENT_RATE	Determines the minimum content rate (in kbps) required for endpoints to share H.264 high quality content via the Content channel When Content Setting is Live Video. Range: 0-1536 Default: 384
H323_FREE_VIDEO_RESOURC ES	For use in the Avaya Environment. In the Avaya Environment there are features that involve converting undefined dial-in participants' connections from video to audio (or vice versa). To ensure that the participants' video resources remain available for them, and are not released for use by Audio Only calls, set this flag to NO. If set to YES, the Collaboration Server will release video resources for <i>Audio Only</i> calls. Default: YES.
HIDE_CONFERENCE_PASSWO RD	 If set to YES (default in Ultra Secure Mode): Conference and Chairperson Passwords that are displayed in the Collaboration Server Web Client or RMX Manager are hidden when viewing the properties of the conference. Automatic generation of passwords (both conference and chairperson passwords) is disabled, regardless of the settings of the flags: NUMERIC_CONF_PASS_DEFAULT_LEN NUMERIC_CHAIR_PASS_ DEFAULT_LEN. For more information see Automatic Password Generation Flags. Default: NO.
IP_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 from 1920Kbps to 18432, 100bits/sec to match the actual rate of the IP Only HD Video Switching conference running on the MGC. Note: If the flag MIX_LINK_ENVIRONMENT is set to NO, the IP_ENVIRONMENT_LINK flag must be set to YES.

Flag	Description
IP_RESPONSE_ECHO	When the <i>System Flag</i> value is YES , the Collaboration Server will respond to <i>ping</i> (<i>IPv4</i>) and <i>ping6</i> (<i>IPv6</i>) commands. When set to NO , the Collaboration Server will not respond to <i>ping</i> and <i>ping6</i> commands.
ITP_CERTIFICATION	When set to NO (default), this flag disables the telepresence features in the Conference Profile. Set the flag to YES to enable the telepresence features in the Conference Profile (provided that the appropriate License is installed).
LAN_REDUNDANCY	Enables Local Area Network port redundancy on RealPresence Collaboration Server (RMX) 2000/4000 RTM LAN Card and RealPresence Collaboration Server (RMX) 1500 LAN ports on the RTM IP 1500. Default: NO Range: YES / NO Note: If the flag value is set to YES and either of the LAN connections (LAN1 or LAN2) experiences a problem, an active alarm is raised stating that there is no LAN connection, specifying both the card and port number.
LIMIT_SD_AND_CIF_BW_MPMR X	When to YES (default), limits the maximum negotiated and opened bit rate for resolutions equal or lower than SD to 1Mbps. When set to NO no limitation is applicable to SD and CIF bit rates. Range: YES/NO. Default: YES.
MANAGE_TELEPRESENCE_RO OM_SWITCH_LAYOUTS	Determines whether the MLA or the RMX controls the Room Switch Telepresence Layouts. When set to NO, the RMX does not manage Telepresence Room Switch Layouts and they continue to be managed by the MLA. When set to YES, the RMX manages Telepresence Room Switch Layouts. Default: NO Range: YES / NO Note: System re-start is not required for this flag's settings to take effect. For more information see Room Switch Telepresence Layouts.
MAX_ALLOWED_RTV_HD_FRA ME_RATE	Defines the threshold Frame Rate (fps) in which RTV Video Protocol initiates HD resolutions. Flag values are as follows: Range: 0-30 (fps) Default: 0 (fps) - Implements any Frame Rate based on Lync RTV Client capabilities

Flag	Description
MAX_RTV_RESOLUTION	Enables you to override the Collaboration Server resolution selection and limit it to a lower resolution, hence minimizing the resource usage to 1 or 1.5 video resources per call instead of 3 resources. Possible flag values are: AUTO (default), QCIF, CIF, VGA or HD720.
MAX_TRACE_LEVEL	This flag indicates the debugging level for system support. The flag's values have been modified for version 7.8 and is not backward compatible with previous versions. Possible values: From version 7.8 - TRACE = t, DEBUG = d, INFO_NORMAL = n, INFO_HIGH = i, WARN = w, ERROR = e, FATAL = f, OFF = o. From version 7.7 or lower - TRACE = n/a, DEBUG = n/a, INFO_NORMAL = n, INFO_HIGH = api, WARN = n/a, ERROR = crt, FATAL = n/a, OFF = no. Default: n
MAXIMUM_RECORDING_LINKS	The maximum number of Recording Links available for selection in the Recording Links list and the Conference Profile - Recording dialog box. Range: 1 - 100 Default: 20
MEDIA_NIC_MTU_SIZE	MTU size (Maximum Transmission Unit controls the maximum data payload size (bytes) transmitted in a single packet over the network. The Collaboration Server sends large amount of data over the network and may be required to adjust its MTU size according to the network environment in which it is deployed. MTU configuration is applicable to Collaboration Servers with RTM-LAN cards installed only. Default: 1500
MIN_H239_HD1080_RATE	Used to set the threshold line rate for HD Resolution Content: the line rate at which the Collaboration Server will send Content at HD1080 Resolution. Setting the flag to 0 disables HD Resolution Content. Default: 768 kbps.
MINIMUM_FRAME_RATE_THRE SHOLD_FOR_SD	Low quality, low frame rate video is prevented from being sent to endpoints by ensuring that an SD channel is not opened at frame rates below the specified value. Range: 0 -30 Default: 15
MIX_LINK_ENVIRONMENT	In H.239-enabled MIH Cascading, when MGC is on level 1, setting this flag to YES will adjust the line rate of HD Video Switching conferences run on the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 from 1920Kbps to 17897, 100bits/sec to match the actual rate of the HD Video Switching conference running on the MGC. Note: If the flag MIX_LINK_ENVIRONMENT is set to YES, the IP_ENVIRONMENT_LINK flag must be set to NO.

Flag	Description
MS_CAC_AUDIO_MIN_BR	The minimum bit rate for audio using the Microsoft CAC (Call Admission Control) protocol. When the bit rate is lower than the MS_CAC_AUDIO_MIN_BR, the call is not connected. Range: 0 - 384 Default: 30
MS_CAC_VTDEO_MIN_BR	The minimum bit rate for video using the Microsoft CAC (Call Admission Control) protocol. When the bit rate is lower than the MS_CAC_VIDEO_MIN_BR, the call is not connected as a video call Range: 0 - 384 Default: 40
MS_KEEP_ALIVE_ENABLE	Enables the Microsoft keep alive flag. Set it YES to ensure that endpoints such as HDX remain connected to the conference for its duration when the Collaboration Server is configured with FQDN address and the Lync server is working with load balancing and holds more than one address. Range: YES/NO Default: NO Note:Beginnig with version 8.1, the functionality of the MS_KEEP_ALIVE_ENABLE System Flag has been replaced with the following System Flags: SIP_TCP_KEEP_ALIVE_TYPE SIP_TCP_KEEP_ALIVE_BEHAVIOR For more information see FW (Firewall) NAT Keep Alive.
MS_PROXY_REPLACE	Enables the <i>proxy=replace</i> parameter in the <i>SIP Header</i> . When set to YES the outbound proxy to replaces the contact information in the contact header with its own enabling other clients and servers to reach the client using the proxy's <i>IP</i> address, even if the client is behind a firewall. Possible Values: YES / NO Default: YES
NETWORK_IND_CRITICAL_PER CENTAGE	The percentage degradation due to packet loss required to change the indicator from <i>Major</i> to <i>Critical</i> . Default: 5
NETWORK_IND_MAJOR_PERC ENTAGE	The percentage degradation due to packet loss required to change the indicator from <i>Normal</i> to <i>Major</i> . Default: 1
NUM_OF_INITIATE_HELLO_ME SSAGE_IN_CALL_ESTABLISHM ENT	Indicates how many times the Hello (keep alive) message is sent from the Collaboration Server to the endpoint in an environment that includes a Session Border Controller (SBC) with a 3-second interval between messages. Range: 1 to 10. Default:3

Flag	Description
NUM_OF_PCM_IN_MPMX	In Collaboration Server 1500/2000/4000 systems with MPMx cards, sets the maximum number of PCM sessions. The default value of this flag is set according to the SVC license: 1 - If SVC is enabled in the license (the only possible value). 4 - If SVC is disabled in the license Range: 1-4 (If SVC is disabled in the license).
NUMBER_OF_REDIAL	Enter the number re dialing attempts required. Dialing may continue until the conference is terminated. Default: 3
OCSP_RESPONDER_TIMEOUT	Not Supported in RMX 1800. Determines the number of seconds the RMX is to wait for an OCSP response from the OCSP Responder before failing the connection. Network latency or slow WAN links can cause login problems when logging in to the RMX's Management Network. This System Flag's value determines the number of seconds the MCU is to wait for an OCSP response from the OCSP Responder before failing the connection. Default: 3 (seconds) Range: 1-20 (seconds)
PARTY_GATHERING_DURATIO N_SECONDS	The value of this <i>System Flag</i> sets the duration, in seconds, of the display of the <i>Gathering</i> slide for participants that connect to the conference after the conference start time. Range: 0 - 3600 Default: 15 For more information see Video Preview (AVC Participants Only).
PASSWORD_FAILURE_LIMIT	The number of unsuccessful Logins permitted in Ultra Secure Mode. Default: 3
PCM_FECC	Determines whether the DTMF Code, ##, the Far/Arrow Keys (FECC) or both will activate the PCM interface. This flag can be also be used in combination with DTMF code definitions to disable PCM. Possible Values: YES / NO Default: YES.
PCM_LANGUAGE	Determines the language of the PCM interface. Possible Values are: ENGLISH, CHINESE_SIMPLIFIED, CHINESE_TRADITIONAL, JAPANESE, GERMAN, FRENCH, SPANISH, KOREAN, PORTUGUESE, ITALIAN, RUSSIAN, NORWEGIAN Default: Current Collaboration Server Web Client language.
PORT_GAUGE_ALARM	When set to YES, if system resource usage reaches the High Port Usage Threshold as defined for the Port Gauges, System Alerts in the form of an Active Alarm and an SNMP trap are generated.

Flag	Description
PRESERVE_ICE_CHANNEL_IN_ CASE_OF_LOCAL_MODE	When set to NO (default), local the ICE channel is closed after applying CAC bandwidth management when Call Admission Control is enabled in the local network. When set to YES, the ICE channel is preserved open throughout the call. Default: NO
PRESERVE_PARTY_CELL_ON_ FORCE_LAYOUT	Used to prevent reassignment of cells in a forced layout that were assigned to endpoints that have disconnected, paused their video, or have been removed from the conference. The cell will remain black until the endpoint reconnects or a new layout is used, or the conference ends. Range: YES / NO Default: NO • NO - Cells of dropped endpoints are reassigned. Endpoints that reconnect will be treated as new endpoints. • YES - Cells of dropped endpoints are not reassigned, but will be reserved until the endpoint reconnects. For information see the <i>Polycom RealPresence Collaboration Server (RMX)</i> 1500/1800/2000/4000 Getting Started Guide, Force Layout and Preserve Participant Call.
PSTN_RINGING_DURATION_SE CONDS	If there is a slow response from the <i>ISDN</i> switch, the <i>PSTN</i> dial-out ringing duration (in seconds) is used by the Collaboration Server to disconnect the call. Default: 45
QOS_IP_AUDIO	Used to select the priority of audio packets when <i>DiffServ is</i> the is the selected method for packet priority encoding. Default: 0x31
QOS_IP_VIDEO	Used to select the priority of video packets when <i>DiffServ is</i> the is the selected method for packet priority encoding. Default: 0x31
QOS_MANAGEMENT_NETWOR	Enter the <i>DSCP</i> value for the <i>RMX Management Network</i> . Default: 0x10 Range: 0x00 - 0x3F
REDUCE_CAPS_FOR_REDCOM _SIP	To accommodate deployments where some devices have limits on the size of the SDP payload in SIP messages (such as LSCs from Redcom running older software versions), when the flag value = YES, the SDP size is less than 2kb and includes only one audio and one video media line. Default: NO
REDIAL_INTERVAL_IN_SECON DS	Enter the number of seconds that the Collaboration Server should wait before successive re dialing attempts. Range: 0-30 (Default: 10)

Flag	Description
REDUCE_CAPS_FOR_REDCOM _SIP	To accommodate Redcom's SDP size limit, when the flag value = YES, the SDP size is less than 2kb and includes only one audio and one video media line. Default: NO
REJECT_INCORRECT_PRECED ENCE_DOMAIN_NAME	When set to YES, when the Precedence Domain of a SIP dial-in call does not match the Precedence Domain of the RMX, the call is rejected. For more information, see MLPP (Multi Level Precedence and Preemption). Possible values: YES/NO Default: No
REMOVE_H323_EPC_CAP_TO_ NON_POLYCOM_VENDOR	Used to disable <i>EPC</i> protocol. Use of <i>Polycom's</i> proprietary protocol, <i>High Profile</i> , <i>EPC</i> , may result in interoperability issues when used with other vendors' endpoints. Possible values: YES / NO Default: NO
REMOVE_H323_HIGH_PROFILE _CAP_TO_NON_POLYCOM_VE NDOR	Used to disable <i>High Profile</i> protocol. Use of <i>Polycom's</i> proprietary protocol, <i>High Profile</i> , may result in interoperability issues when used with other vendors' endpoints. Possible values: YES / NO Default: NO
REMOVE_H323_HIGH_QUALITY _AUDIO_CAP_TO_NON_POLYC OM_VENDOR	Used to disable the following Audio Codecs: G231 G7221C G7221 G719 Siren22 Siren14 Possible values: YES / NO Default: NO
REMOVE_H323_LPR_CAP_TO_ NON_POLYCOM_VENDOR	Used to disable <i>H.323 LPR</i> protocol. Use of <i>Polycom's</i> proprietary protocol, <i>H.323 LPR</i> , may result in interoperability issues when used with other vendors' endpoints. Possible values: YES / NO Default: NO
REMOVE_IP_IF_NUMBER_EXIS TS	Between the time a conference is scheduled and when it becomes active, the IP of an endpoint may change, especially in an environment that uses DHCP. This flag determines if the <i>E.164</i> number is to be substituted for the IP address in the dial string. Range: YES / NO Default: YES - The IP address will be substituted with the E.164 number.

Flag	Description
RFC2833_DTMF	Controls the receipt of in-band and out-of-band DTMF Codes. When set to: • YES The RMX will receive DTMF Codes sent in-band. • NO The RMX receive DTMF Codes sent out-of-band. The RMX always sends DTMF Codes in-band (as part of the Audio Media stream). Range: YES/NO Default YES
RMX_MANAGEMENT_SECURIT Y_PROTOCOL	Enter the protocol to be used for secure communications. Default: TLSV1_SSLV3 (both). Default for U.S. Federal licenses: TLSV1.
RTCP_FIR_ENABLE	When set to YES, the <i>Full Intra Request</i> (<i>FIR</i>) is sent as <i>INFO</i> (and not <i>RTCP</i>). Default = YES
RTCP_FLOW_CONTROL_TMMB R_ENABLE	Enables/disables the SIP RTCP flow control parameter. Default: YES
RTCP_FLOW_CONTROL_TMMB R_INTERVAL	Modifies the interval (in seconds) of the TMMBR (Temporary Maximum Media Stream Bit Rate) parameter for SIP RTCP flow control. Range: 5 - 999 (seconds) Default: 180
RTCP_PLI_ENABLE	When set to YES, the (Picture Loss Indication (<i>PLI</i>) is sent as <i>INFO</i> (and not <i>RTCP</i>). Default = YES
RTCP_QOS_IS_EQUAL_TO_RT P	Range: YES/NO Default: YES
SELF_IND_LOCATION	Change the location of the display of the Network Quality Indicator of the participant's own endpoint. Default: BOTTOM_RIGHT Range: TOP_LEFT TOP TOP_RIGHT BOTTOM_LEFT BOTTOM BOTTOM_RIGHT

Flag	Description
SEND_SIP_BUSY_UPON_RESO URCE_THRESHOLD	When set to YES , it enables the Collaboration Server to send a busy notification to a SIP audio endpoint or a SIP device when dialing in to the Collaboration Server whose audio resource usage exceeded the Port Usage threshold. When set to NO , the system does limit the SIP audio endpoint connections to a certain capacity and will not send a busy notification when the resource capacity threshold is exceeded. Default: NO
SEND_SRTP_MKI	Enables or disables the inclusion of the <i>MKI</i> field in <i>SRTP</i> packets sent by the Collaboration Server. Setting the value to NO to disables the inclusion of the <i>MKI</i> field in <i>SRTP</i> packets sent by the Collaboration Server. Set this flag to: NO Men all conferences on the <i>RMX</i> will not have <i>MS-Lync</i> clients participating and will have 3rd party endpoints participating. When using endpoints (eg. <i>CounterPath Bria 3.2 Softphone</i>) that cannot decrypt <i>SRTP</i> -based audio and video streams if the <i>MKI</i> (<i>Master Key Identifier</i>) field is included in <i>SRTP</i> packets sent by the Collaboration Server. This setting is recommended for <i>Maximum Security Environments</i> . YES When any conferences on the <i>RMX</i> will have both <i>MS-Lync</i> clients and <i>Polycom</i> endpoints participating. Some 3rd party endpoints may be unsuccessful in participating in conferences with this setting. Notes: This <i>System Flag</i> must be added and set to YES (default) when <i>Microsoft Office Communicator</i> and <i>Lync Clients</i> are used as they all support <i>SRTP</i> with <i>MKI</i> . The system flag must be added and set to NO when Siemens phones (<i>Openstage</i> and <i>ODC WE</i>) are used in the environment as they do not support <i>SRTP</i> with <i>MKI</i> .
SEND_WIDE_RES_TO_IP	When set to YES (default), the Collaboration Server sends wide screen resolution to IP endpoints. Endpoint types that do not support wide screen resolutions are automatically identified by the Collaboration Server according to their product type and version and will not receive the wide resolution even when the flag is set to YES. When manually added and set to NO , the Collaboration Server does not send wide screen resolution to all IP endpoints. Default: YES.

Flag	Description
SEND_WIDE_RES_TO_ISDN	When set to YES , the Collaboration Server sends wide screen resolution to ISDN endpoints. When set to NO (default), the Collaboration Server does not send wide
	screen resolution to ISDN endpoints. Default: NO.
SET_AUDIO_CLARITY	Audio Clarity improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity. The enhancement is applied to the following low bandwidth (4kHz) audio algorithms: • G.729a • G.711 • Guidelines Note: This flag sets the initial value for Audio Clarity during First-time Power-up. Thereafter the feature is controlled via the New Profile - Audio Settings dialog box. Possible Values: ON / OFF Default: OFF For more information see Defining New Profiles.
SET_AUDIO_PLC	Packet Loss Concealment (PLC) for Siren audio algorithms improves received audio when packet loss occurs in the network. The following audio algorithms are supported: • Siren 7 (mono) • Siren 14 (mono/stereo) • Siren 22 (mono/stereo) Possible Values: ON / OFF Default: ON Note: The speaker's endpoint must use a Siren algorithm for audio compression.
SET_AUTO_BRIGHTNESS	Auto Brightness detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout. Auto Brightness only increases brightness and does not darken video windows. Note: This flag sets the initial value for Auto Brightness during First-time Power-up. Thereafter the feature is controlled via the New Profile - Video Quality dialog box. Possible Values: YES / NO Default: NO For more information see Defining New Profiles.

Flag	Description
SET_DTMF_SOURCE_DIFF_IN_ SEC	If the ACCEPT_VOIP_DTMF_TYPE flag is set to 0 (Auto) this flag determines the interval, in seconds after which the Collaboration Server will accept both <i>DTMF</i> tones (inband) and digits (outband). Default: 120
SIP_BFCP_DIAL_OUT_MODE	Controls BFCP's use of UDP and TCP protocols for dial-out SIP Client connections according to its value: • AUTO (Default) If SIP Client supports UDP, TCP or UDP and TCP: - BFCP/UDP is selected as Content sharing protocol. • UDP If SIP Client supports UDP or UDP and TCP: - BFCP/UDP selected as Content sharing protocol. If SIP Client supports TCP - Cannot share Content. • TCP If SIP Client supports TCP or UDP and TCP - BFCP/TCP selected as Content sharing protocol. If SIP Client supports UDP - Cannot share Content.
SIP_DUAL_DIRECTION_TCP_C ON	In environments set to integration with Microsoft, if set to YES the system sends a new request on the same TCP connection (instead of opening a new one).
SIP_ENABLE_FECC	By default, FECC support for SIP endpoints is enabled at the MCU level. You can disable it by manually adding this flag and setting it to NO.
SIP_FAST_UPDATE_INTERVAL_ ENV	Default setting is 0 to prevent the Collaboration Server from automatically sending an Intra request to all SIP endpoints. Enter n (where n is any number of seconds other than 0) to let the Collaboration Server automatically send an Intra request to all SIP endpoints every n seconds. It is recommended to set the flag to 0 and modify the frequency in which the request is sent at the endpoint level (as defined in the next flag).
SIP_FAST_UPDATE_INTERVAL_ EP	Default setting is 6 to let the Collaboration Server automatically send an Intra request to Microsoft OC endpoints only, every 6 seconds. Enter any other number of seconds to change the frequency in which the Collaboration Server send the Intra request to Microsoft OC endpoints only. Enter 0 to disable this behavior at the endpoint level (not recommended).

Flag	Description
SIP_FORMAT_GW_HEADERS_F OR_REDCOM	Controls whether the <i>RMX</i> adds special gateway prefix and postfix characters to the user portion of the <i>SIP URI</i> expressed in the " <i>From</i> " and " <i>Contact</i> " headers of <i>SIP</i> messages sent during calls involving <i>Gateway Services</i> . The addition of these characters can result in call failures with some <i>SIP</i> call servers. It is recommended to set this flag to YES whenever the <i>RMX</i> is deployed such that it registers its conferences to a <i>SIP</i> call server. Range: YES, NO Default: NO
SIP_FREE_VIDEO_RESOURCE S	For use in Avaya and Microsoft Environments. When set to NO (required for Avaya and Microsoft environments), video resources that were allocated to participants remain allocated to the participants as long as they are connected to the conference even if the call was changed to audio only. The system allocates the resources according to the participant's endpoint capabilities, with a minimum of 1 CIF video resource. Enter YES to enable the system to free the video resources for allocation to other conference participants. The call becomes an audio only call and video resources are not guaranteed to participants if they want to add video again. Default value in Microsoft environment: NO.
SIP_TCP_PORT_ADDR_STRAT EGY	Setting the flag to 1 prevents the use of two sockets for one SIP call - one for inbound traffic, one for outbound traffic. This is done by inserting port "5060/5061" into the Route[0] header. Possible values: 0 - Inbound traffic on port 5060/5061 outbound traffic on port 60000 1 - Both inbound and outbound traffic on port 5060/5061 Default: 1
SITE_NAME_TRANSPARENCY	This flag is not supported from version 8.1. This function is controlled using the <i>Profile -Site Names</i> dialog box.
SITE_NAMES_ALWAYS_ON	This flag is not supported from version 8.1. This function is controlled using the <i>Profile -Site Names</i> dialog box.
SOCKET_ACTIVITY_TIMEOUT	For use in Microsoft environments. When the MS_KEEP_ALIVE System Flag is set to YES, the value of this flag is used as the MS Keep-Alive Timer value.
SUPPORT_HIGH _PROFILE	Enables or disables the support of <i>High Profile</i> video protocol in CP conferences. This flag is specific to CP conferences and has no effect on VSW conferences. Range: YES / NO Default: YES

Flag	Description
SUPPORT_HIGH _PROFILE_WITH_ISDN	Enables or disables the support of <i>High Profile</i> video protocol for ISDN participants in CP conferences. This flag is specific to CP conferences and has no effect on VSW conferences. Range: YES / NO Default: NO
TC_BURST_SIZE	This flag regulates the Traffic Control buffer or maxburst size as a percentage of the participant line rate. Range: 1-30.
TC_LATENCY_SIZE	This flag limits the latency (in milliseconds) or the number of bytes that can be present in a queue. Range: 1-1000 (in milliseconds).
TCP_RETRANSMISSION_TIME OUT	The number of seconds the server will wait for a <i>TCP</i> client to answer a call before closing the connection. Default = 5 (seconds)
V35_MULTIPLE_SERVICES	Not Supported in RMX 1800. If the connection of multiple Serial Gateways to RTM-LAN cards is required: The V35_MULTIPLE_SERVICES System Flag must be set to YES. The default value of the V35_MULTIPLE_SERVICES System Flag is NO, enabling only one Serial Gateway to be supported per RTM-LAN card.
V35_ULTRA_SECURED_SUPPO RT	This flag must be set to YES when deploying a Serial Gateway S4GW in Ultra Secure Mode
VSW_CIF_HP_THRESHOLD_BI TRATE	Controls the <i>Minimum Threshold Line Rate</i> (kbps) for <i>CIF</i> resolution for <i>High Profile-enabled VSW conferences</i> . Default: 64
VSW_HD1080p_HP_THRESHOL D_BITRATE	Controls the <i>Minimum Threshold Line Rate</i> (kbps) for <i>HD1080p</i> resolution for <i>High Profile-enabled VSW conferences</i> . Default: 1024
VSW_HD720p30_HP_THRESHO LD_BITRATE	Controls the <i>Minimum Threshold Line Rate</i> (kbps) for <i>HD720p30</i> resolution for <i>High Profile-enabled VSW conferences</i> . Default: 512
VSW_HD720p50-60_HP_THRES HOLD_BITRATE	Controls the <i>Minimum Threshold Line Rate</i> (kbps) for <i>HD720p50</i> and <i>HD720p50</i> resolutions for <i>High Profile-enabled VSW conferences</i> . Default: 832

Flag	Description
VSW_RATE_TOLERANCE_PER ECENT	Determines the percentage of bandwidth that can be deducted from the required bandwidth to allow participants to connect to the conference.
	For example, a value of 20 will allow a participant to connect to the conference if the allocated line rate is up to 20% lower than the conference line rate (or between 80% to 100% of the required bandwidth). Range: 0 - 75 Default: 0
VSW_SD_HP_THRESHOLD_BIT RATE	Controls the <i>Minimum Threshold Line Rate</i> (kbps) for <i>SD</i> resolution for <i>High Profile-enabled VSW conferences</i> . Default: 128
WRONG_NUMBER_DIAL_ RETRIES	The number of re-dial attempts for a wrong destination number or a wrong destination number time-out. Range: 0 - 5 Default: 3 A flag value of 0 means that no redials are attempted.

Manually Adding Flags to the CS_MODULE_PARAMETERS Tab

Using the procedure to manually add flags to the System Configuration, the following flags can be manually added to the **CS_MODULE_PARAMETERS** tab:

Manually Added CS_MODULE_PARAMETERS System Flags

Flag	Description
CS_ENABLE_EPC	Add this flag with the value YES (default value is NO) to enable endpoints that support People+Content and require a different signaling (for example, FX endpoints) to receive Content.
H245_TUNNELING	For use in the Avaya Environment. In the Avaya Environment, set the flag to YES to ensure that H.245 is tunneled through H.225. Both H.245 and H.225 will use the same signaling port. Default: NO.
H323_RAS_IPV6	If the Collaboration Server is configured for <i>IPv4 & IPv6</i> addressing, <i>RAS</i> (<i>Registration</i> , <i>Admission</i> , and <i>Status</i>) messages are sent in both <i>IPv4</i> and <i>IPv6</i> format. If the gatekeeper cannot operate in <i>IPv6</i> addressing mode, registration fails and endpoints cannot connect using the Collaboration Server prefix. In such cases this <i>System Flag</i> should be set to NO . Default: YES

Manually Added CS_MODULE_PARAMETERS System Flags

Flag	Description
H323_TIMERS_SET_I NDEX	Enables or disables H.323 index timer according to standard or proprietary H.323 protocol. Possible values: 0 (Default) - Sets the H.323 index timer to Polycom proprietary. 1 - Sets the H.323 index timer based on the H.323 Standard recommendation. Note: For homologation and certification testing, this flag must be set to 1.
MS_UPDATE_CONTAC T_REMOVE	 When the flag value is set to: YES - The Contact Header is removed from the UPDATE message that is sent periodically to the endpoints. This is required when the SIP Server Type field of the IP Network Service is set as Microsoft. Removal of the Contact Header from the UPDATE message is required specifically by OCS R2. NO - The Contact Header is included in the UPDATE message. This is the system behavior when the SIP Server Type is set as Generic. This is required when the Collaboration Server is configured to accept calls from both Microsoft LYNC and Cisco CUCM as CUCM requires the Contact Header.
QOS_IP_SIGNALING	Used to select the priority of IP packets when <i>DiffServ is</i> the is the selected method for packet priority encoding. Range: 0x## Default: 0x28
SIP_DUAL_DIRECTIO N_TCP_CON	For use in Microsoft environments. When set to YES, sends a new request on the same TCP connection instead of opening a new connection. Range: YES/NO Default: NO
SIP_ST_ENFORCE_VA L	For use in Microsoft environments. Session timer interval in seconds. Default = YES
SIP_TCP_TLS_TIMER S	Determines the timeout characteristics of SIP TCP TLS connections. Format: SIP_TCP_TLS_TIMERS = <string> The string contains the following parameters: Ct - Timeout of TCP CONNECT operation (seconds) Cs - Timeout of TLS CONNECT operation (seconds) A - Timeout of accept operation (seconds) D - Timeout of disconnect operation (nanoseconds) H - Timeout of handshake operation (seconds) Default: <1,5, 4,500000,5></string>

Manually Added CS_MODULE_PARAMETERS System Flags

Flag	Description
SIP_TIMERS_SET_IND EX	SIP Timer type timeout settings according to standard or proprietary protocol. Possible values are: 0 - Default 1 - SIP Standard recommendation. Note: For homologation and certification testing, this flag must be set to 1.
SIP_TO_TAG_CONFLI CT	For use in Microsoft environments. In case of forking, a tag conflict will be resolved when Status 200 OK is received from an answering UA. Default: YES

Deleting a Flag

To delete a flag:

- 1 In the System Flags dialog box, select the flag to delete and click the Delete Flag button.
- 2 In the confirmation message box, click **Yes** to confirm.
- 3 Click OK to close the System Flags dialog box.

Auto Layout Configuration

The **Auto Layout** option lets the Collaboration Server automatically select the conference video layout based on the number of participants currently connected to the conference. You can modify the default selection of the conference video layout to customize it to your conferencing preferences.

Customizing the Default Auto Layout

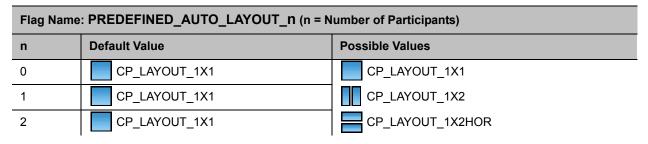
The default **Auto Layout** is controlled by 13 flags:

PREDEFINED AUTO LAYOUT 0, ..., PREDEFINED AUTO LAYOUT 12

Each of the 11 **Auto Layout** flags can be left at its default value, or set to any of the **Possible Values** listed in the following **Default Auto Layouts** table.

The flag that controls the **Auto Layout** you wish to modify must be added to the **System Configuration** file. For more information see Manually Adding and Deleting System Flags.

Default Auto Layouts



Default Auto Layouts

Flag Name: PREDEFINED_AUTO_LAYOUT_n (n = Number of Participants)		
n	Default Value	Possible Values
3	CP_LAYOUT_1x2VER	□□ CP_LAYOUT_1X2VER
4	CP_LAYOUT_2X2	CP_LAYOUT_2X1
5	CP_LAYOUT_2X2	CP_LAYOUT_1P2HOR
6	CP_LAYOUT_1P5	CP_LAYOUT_1P2HOR_UP
7	CP_LAYOUT_1P5	CP_LAYOUT_1P2VER
8	CP_LAYOUT_1P7	CP_LAYOUT_2X2
9	CP_LAYOUT_1P7	CP_LAYOUT_1P3HOR_UP
10	CP_LAYOUT_1P7	CP_LAYOUT_1P3VER
11	CP_LAYOUT_2P8	CP_LAYOUT_1P4HOR
12	CP_LAYOUT_1P12	CP_LAYOUT_1P4HOR_UP
		CP_LAYOUT_1P4VER
		CP_LAYOUT_1P5
		CP_LAYOUT_1P7
		CP_LAYOUT_1P8UP
		CP_LAYOUT_1P8CENT
		CP_LAYOUT_1P8HOR_UP
		CP_LAYOUT_3X3
		CP_LAYOUT_2P8
		CP_LAYOUT_1P12
		CP_LAYOUT_4X4

Example:

The following table illustrates the effect of modifying the PREDEFINED_AUTO_LAYOUT_5 flag in conferences with fewer or more participants than the number of windows selected in the default layout.

Example of Predefined Auto Layouts

Flag	Set to Possible Value	Number of Participants	Participant's View
	CP_LAYOUT_ 1x2VFR	3	Voice activated switching displays the current speaker in the left window of the video layout and only the two last speakers are displayed.
PREDEFINED		7	
_AUTO_LAYOUT_5	CP_LAYOUT _IP5	3	
			Voice activated switching displays the current speaker in the large (top left) window of the video layout.
		7	Voice activated switching displays the current speaker in the top left window of the video layout.

LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag Values

The following table lists the value for each video layout that can be defined for the LEGACY_EP_CONTENT_DEFAULT_LAYOUT Flag. It allows the selection of video layout that will be displayed on the screen of the legacy endpoint when switching to Content mode.

Legacy Endpoint Content Default Layout Flag Values

Layout	Flag Value
	CP_LAYOUT_1X1
	CP_LAYOUT_1X2
	CP_LAYOUT_1X2HOR

Legacy Endpoint Content Default Layout Flag Values

Layout	Flag Value
	CP_LAYOUT_1X2VER
	CP_LAYOUT_2X1
	CP_LAYOUT_1P2HOR
	CP_LAYOUT_1P2HOR_UP
	CP_LAYOUT_1P2VER
	CP_LAYOUT_2X2
	CP_LAYOUT_1P3HOR_UP
	CP_LAYOUT_1P3VER
0000	CP_LAYOUT_1P4HOR_UP
	CP_LAYOUT_1P4HOR
	CP_LAYOUT_1P4VER
	CP_LAYOUT_1P5
0000	CP_LAYOUT_1P7
	CP_LAYOUT_1P8UP
0000	CP_LAYOUT_1P8CENT
0000	CP_LAYOUT_1P8HOR_UP
000 000	CP_LAYOUT_3X3
	CP_LAYOUT_2P8
	CP_LAYOUT_1P12
0000 0000 0000	CP_LAYOUT_4X4

CS_ENABLE_EPC Flag

Endpoints that support **People+Content** may require a different signaling (for example, FX endpoints). For these endpoints, manually add the flag **CS_ENABLE_EPC** with the value YES (default value is NO) to the **CS_MODULE_PARAMETERS** tab.

Automatic Password Generation Flags

The Collaboration Server can be configured to automatically generate conference and chairperson passwords when the **Conference Password** and **Chairperson Password** fields are left blank.

Guidelines

- If the flag HIDE_CONFERENCE_PASSWORD is set to YES, the automatic generation of passwords (both conference and chairperson passwords) is disabled, regardless of the settings of the flags NUMERIC_CONF_PASS_DEFAULT_LEN and NUMERIC_CHAIR_PASS_DEFAULT_LEN.
- The automatic generation of conference passwords is enabled/disabled by the flag NUMERIC_CONF_PASS_DEFAULT_LEN.
- The automatic generation of chairperson passwords is enabled/disabled by the flag NUMERIC_CHAIR_PASS_ DEFAULT _LEN.
- The automatically generated passwords will be numeric and random.
- The passwords are automatically assigned to ongoing conferences, Reservations, and Meeting Rooms at the end of the creation process (once they are added to the Collaboration Server).
- Automatically assigned passwords can be manually changed through the Conference/Meeting Room/Reservation Properties dialog boxes.
- Deleting an automatically created password will not cause the system to generate a new password and the new password must be added manually or the field can be left blank.
- If a password was assigned to the conference via Microsoft Outlook using the PCO add-in, the system does not change these passwords and additional passwords will not be generated (for example, if only the conference password was assigned a chairperson password will not be assigned).
- If the flag values (i.e. the password lengths) are changed, passwords that were already assigned to conferences, Reservations, and Meeting Rooms will not change and they can be activated using the existing passwords. Only new conferencing entities will be affected by the change.



Do not enable this option in an environment that includes a *Polycom DMA* system.

Enabling the Automatic Generation of Passwords

To enable the automatic generation of passwords, the following flags have to be defined:

Automatic Password Generation Flags

Flag	Description
HIDE_CONFERENCE_PASSWORD	NO (default) - Conference and chairperson passwords are displayed when viewing the Conference/Meeting Room/ Reservation properties. It also enables the automatic generation of passwords in general.
	Yes - Conference and Chairperson Passwords are hidden (they are replaced by asterisks). It also disables the automatic generation of passwords.

Flag	Description
NUMERIC_CONF_PASS_MIN_LEN	Enter the minimum number of characters required for conference passwords. Possible values: 0 – 16 .
	0 (default in non-secured mode) means no minimum length. However this setting cannot be applied when the Collaboration Server is in <i>Ultra Secure Mode</i> .
	9 (default in Ultra Secure Mode) Conference password must be at least 9 characters in length.
NUMERIC_CHAIR_PASS_MIN_LEN	Enter the minimum number of characters required for chairperson passwords.
	Possible values: 0 – 16 .
	0 (default in non-secured mode) means no minimum length. However this setting cannot be applied when the Collaboration Server is in <i>Ultra Secure Mode</i> .
	9 (default in Ultra Secure Mode) , Chairperson password must be at least 9 characters in length.
NUMERIC_CONF_PASS_MAX_LEN	Enter the maximum number of characters permitted for conference passwords.
	Possible values: 0 – 16 (non-secured mode) or 9 – 16 (Ultra Secure Mode).
	16 (default) - Conference password maximum length is 16 characters.
NUMERIC_CHAIR_PASS_MAX_LEN	Enter the maximum number of characters permitted for chairperson passwords.
	Possible values: 0 – 16 (non-secured mode) or 9 – 16 (Ultra Secure Mode).
	16 (default) - chairperson password maximum length is 16 characters.
NUMERIC_CONF_PASS_DEFAULT_LEN	This flag enables or disables the automatic generation of conference passwords. The length of the automatically generated passwords is determined by the flag value. Possible values:
	0 – 16, 6 default (non-secured mode)
	 0 and 9 – 16, 9 default (Ultra Secure Mode).
	Enter 0 to disable the automatic generation of passwords.
	Any value other than 0 enables the automatic generation of conference passwords provided the flag HIDE_CONFERENCE_PASSWORD is set to NO.
	If the default is used, in non-secured mode the system will automatically generate conference passwords that contain 6 characters.

Flag	Description
NUMERIC_CHAIR_PASS_ DEFAULT _LEN	This flag enables or disables the automatic generation of chairperson passwords. The length of the automatically generated passwords is determined by the flag value.
	Possible values:
	• 0 - 16, 6 default (non-secured mode)
	 0 and 9 – 16, 9 default (Ultra Secure Mode).
	Enter 0 to disable the automatic generation of passwords.
	Any value other than 0 enables the automatic generation of chairperson passwords provided the flag HIDE_CONFERENCE_PASSWORD is set to NO.
	If the default is used, in non-secured mode the system will automatically generate chairperson passwords that contain 6 characters.

If the default password length defined by the NUMERIC_CONF_PASS_DEFAULT_LEN or NUMERIC_CHAIR_PASS_ DEFAULT LEN does not fall within the range defined by the minimum and maximum length an appropriate fault is added to the Faults list.

Flags Specific to Maximum Security Environments - Ultra Secure Mode

The Collaboration Server can operate in one of two modes: **Standard Security Mode** or **Ultra Secure Mode**.

In **Ultra Secure Mode** the enhanced security features of the version are rigorously enforced.

The **Ultra Secure Mode** is enabled or disabled depending on the value of the **ULTRA_SECURE_MODE System Flag**.

Ultra Secure Mode, is enabled by manually adding the **ULTRA_SECURE_MODE** flag to the **System Configuration** and setting its value to **YES**.

Ultra Secure Mode Flag



WARNING: Once **Ultra Secure Mode** is enabled it can only be undone by performing a **Restore to Factory Defaults**. Also, to implement a Maximum Security environment, other Polycom products on the network must be similarly configured.

For more information see Restoring Defaults.

Ultra Secure Mode



WARNING: Once **Ultra Secure Mode** is enabled it can only be disabled by performing a **Restore to Factory Defaults**. In addition, to implement a *Maximum Security Environment*, other *Polycom* products on the network must be similarly configured.

For more information see the *RealPresence Collaboration Server (RMX) 1500/2000/4000*Deployment Guide for Maximum Security Environments, Restoring the RMX Using the USB Port.

From Version 8.1/8.1.4.J, only MPMx cards are supported.

Ultra Secure Mode is the operating mode of the **RealPresence Collaboration Server** when deployed in a **Maximum Security Environment**. When the **MCU** is set to **Ultra Secure Mode**, all enhanced security features are activated and rigorously enforced.

Enabling Ultra Secure Mode

The **Ultra Secure Mode** is disabled by default and can be enabled by adding the **ULTRA_SECURE_MODE System Flag** and setting its value of to **YES** using the **Setup > System Configuration** menu. Doing so affects the ranges and defaults of other **System Flags** that control:

- Network Security
- User Management
- Strong Passwords
- Login and Session Management
- · Cyclic File Systems alarms

For a detailed description of the installation and configuration of an **MCU** in a **Maximum Security Environment** see the First Time Installation and Configuration chapter of the RealPresence Collaboration Server (RMX) 1500/2000/4000 Deployment Guide for Maximum Security Environments.

ULTRA_SECURE_MODE System Flag

Guidelines

- After modifying the value of the ULTRA_SECURE_MODE System Flag to YES, all Collaboration Server users are forced to change their Login passwords.
- In previous versions the ULTRA_SECURE_MODE System Flag was named JITC_MODE:

- When upgrading from a version that used the JITC_MODE System Flag, the system will automatically create an ULTRA_SECURE_MODE System Flag and set it to the same value as that of the JITC_MODE flag before the upgrade. The system will then delete the JITC_MODE System Flag.
- When downgrading to a version that utilizes the JITC_MODE System Flag, the administrator will need to set the JITC_MODE flag to that of the ULTRA_SECURE_MODE flag before the downgrade.



When the **ULTRA_SECURE_MODE** flag is set to **YES**, the following are not supported:

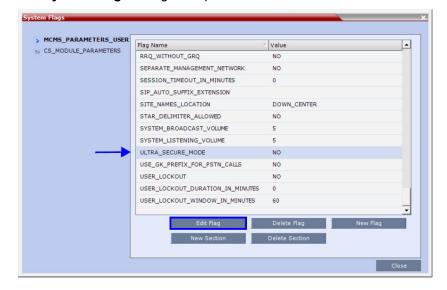
- Connection to Alternate Management Network via LAN3 port
- SUPPORT user
- Auditor user
- Chairperson user
- Connections to External Databases
- IP Sec security protocols
- ISDN Cascade
- PCM

- SSH server
- USB key configuration
- Web link (Hyperlink in Participant Properties dialog box)
- QoS with IPv6
- PCO (MS-Outlook)
- Video Preview
- Serial connection
- Modem connection

To modify the ULTRA_SECURE_MODE System flag value:

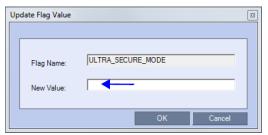
Ultra Secure Mode can be enabled by changing the value of the ULTRA_SECURE_MODE System Flag to YES during First Entry Configuration or at any time using the Setup > System Configuration menu.

1 On the Collaboration Server menu, click Setup > System Configuration. The System Flags dialog box opens.



2 Double-click or select the ULTRA_SECURE_MODE flag and click the Edit Flag button.

3 In the New Value field, enter the flag's new value - YES or NO.



- 4 Click **OK** to close the **Update Flag** dialog box.
- 5 Click **OK** to close the **System Flags** dialog box.



For flag changes (including deletion) to take effect, reset the MCU. For more information see Resetting the Collaboration Server .

System Flags affected by Ultra Secure Mode

When the **ULTRA_SECURE_MODE** flag is set to YES the default and range values of the following flags are affected.

ULTRA_SECURE_MODE Flag Value – Effect on System Flags

	ULTRA_SECURE_MODE =			
Flag	YES		NO	
	Range	Default	Range	Default
Network Security				
ENABLE_ACCEPTING_ICMP_REDIRECT	YES/ NO	NO	YES/ NO	YES
ENABLE_SENDING_ICMP_DESTINATION_UNREACH ABLE	YES/ NO	NO	YES/ NO	YES
SEPARATE_MANAGEMENT_NETWORK	YES/ NO	YES	NO	NO
Login and Session Management				
APACHE_KEEP_ALIVE_TIMEOUT	1-999	15	1-999	120
LAST_LOGIN_ATTEMPTS	YES/ NO	YES	YES/ NO	NO
MAX_KEEP_ALIVE_REQUESTS	0 ->	0		
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER _SYSTEM	4-80	80	4-80	80
MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER	4-80	20	4-80	10

ULTRA_SECURE_MODE Flag Value – Effect on System Flags

	ULTRA_SECURE_MODE =			
Flag	Y	ES	N	10
	Range	Default	Range	Default
SESSION_TIMOUT_IN_MINUTES	1-999	10	0-999	0
USER_LOCKOUT	YES/ NO	YES	YES/ NO	NO
USER_LOCKOUT_DURATION_IN_MINUTES	0-480	0	0-480	0
USER_LOCKOUT_WINDOW_IN_MINUTES	0-45000	60	0-45000	60
User Management			•	
DISABLE_INACTIVE_USER	1-90	30	0-90	0
Strong Passwords				
FORCE_STRONG_PASSWORD_POLICY	YES	YES	YES/NO	NO
HIDE_CONFERENCE_PASSWORD	YES/NO	NO	YES/NO	NO
HIDE_CONFERENCE_PASSWORD	YES/NO	NO	YES/NO	NO
MAX_CONF_PASSWORD_REPEATED_DIGITS	1-4	2	0-4	0
MAX_PASSWORD_REPEATED_CHAR	1-4	2	0-4	2
MIN_PASSWORD_LENGTH	15-20	15	0-20	0
MIN_PWD_CHANGE_FREQUENCY_IN_DAYS	1-7	1	0-7	0
NUM_OF_LOWER_CASE_ALPHABETIC	1-2	2	0-2	0
NUM_OF_NUMERIC	1-2	2	0-2	0
NUMERIC_CHAIR_PASS_MIN_LEN	9-16	9	0-16	0
NUMERIC_CONF_PASS_MIN_LEN	9-16	9	0-16	0
PASS_EXP_DAYS_MACHINE		365		
PASSWORD_EXPIRATION_DAYS	7-90	60	0-90	0
PASSWORD_EXPIRATION_WARNING_DAYS	7-14	7	0-14	0
PASSWORD_HISTORY_SIZE	10-16	10	0-16	0
Cyclic File Systems				
ENABLE_CYCLIC_FILE_SYSTEM_ALARMS	YES/NO	YES	YES/NO	NO

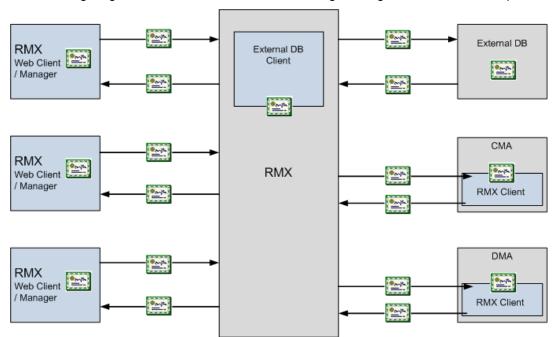
Certificate Management

(PKI) Public Key Infrastructure

PKI (**Public Key Infrastructure**) is a set of tools and policies deployed to enhance the security of data communications between networking entities.

The implementation of PKI on the Collaboration Server has been enhanced to ensure that all networked entities are checked for the presence of unique certificates by implementing the following rules and procedures during the TLS negotiation:

- The Collaboration Server identifies itself with the same certificate when operating as a server and as
 a client.
- The Collaboration Server's management applications: Collaboration Server Web Client and RMX Manager, identify themselves with certificates.
- While establishing the required TLS connection, there is an exchange of certificates between all entities.
- Entities such as CMA and DMA that function as both client and server within the Management Network identify themselves with the same certificate for both their client and server functions.
- A single Certificate Repository is maintained for:
 - The Management Network Service.
 - SIP TLS Personal Certificates for each defined IP Network Service.
 - Trusted (CA) certificate for all TLS connections.
 - CRL for all TLS connections.
- SIP TLS certificates are validated against the CA.
- SIP TLS certificates are managed using CRL and Online Certificate Status Protocol (OCSP).
 - Certificate revocation mode, whether by OCSP or CRL is managed using the i setting of the Management Network.
 - SIP TLS is managed using the General TLS setting.
- The following certificate file formats are supported:
 - ▶ PEM
 - DER
 - PKCS#7/P7B
 - PKCS#12PFX



The following diagram illustrates the certificate exchange during the TLS connection procedure.

Adding Certificates to the Certificate Repository

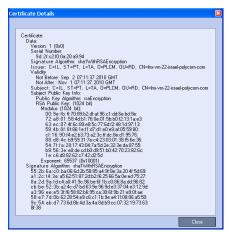
To access the Certification Repository:

In the Collaboration Server Web Client, click Setup > RMX Secured Communication > Certification Repository.

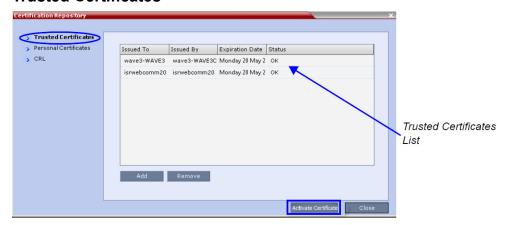
The Certification Repository dialog box contains tabs that display the following lists:

- Trusted Certificates
- Personal Certificates (Management and Signaling Certificates)
- CRL (Certificate Revocation List)

Double-clicking on a certificate in any if the displayed lists, displays the certificate's properties:



Trusted Certificates



By clicking the column headers the Trusted Certificates can be sorted by:

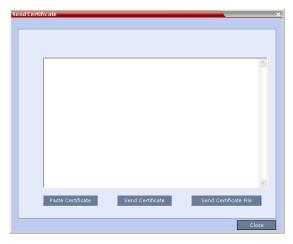
- Issued To
- Issued By
- Expiration Date
- Status

To add a certificate to the repository:

Repeat steps 1 - 2 for each certificate that is to be added to the **Certification Repository**.

1 In the Trusted Certificates tab click the Add button.

The **Send Certificate** dialog box is displayed.



2 Send the certificate to the Collaboration Server.

Two options are available for sending the certificate to the Collaboration Server:

- Paste Certificate and Send Certificate
 Use this option if the certificate has been received from the Certification Authority in text format.
- > Send Certificate File
 Use this option if the certificate has been received from the Certification Authority in file format.

Option. Paste Certificate and Send Certificate

After you have received the certificate from the **Certificate Authority**:

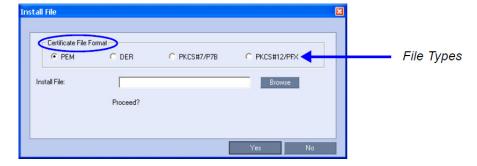
- a Copy (Ctrl + C) the certificate information from the Certificate Authority's e-mail to the clipboard.
- **b** Click **Paste Certificate** to paste the clipboard content into the **Send Certificate** dialog box.
- c Click the **Send Certificate** button to send the certificate to the Collaboration Server.

Option. Send Certificate File

After you have received the certificate file from the **Certificate Authority**:

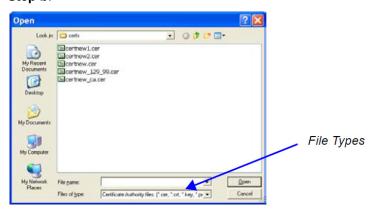
a Click Send Certificate File.

The **Install File** dialog box is displayed.



b Select the Certificate File Format: PEM, DER, PKCS#7/P7B or PKCS#12PFX.

c Enter the certificate file name in the Install File field or click the Browse button.
The Open file dialog box is displayed. The files are filtered according to the file type selected in Step b.



- **d** Enter the certificate file name in the **File name** field or click to select the certificate file entry in the list.
- e Click the Open button.
- f In the Install File dialog box, click the Yes button to proceed.
 The certificate is added to the Trusted Certificate List in the Certification Repository.
- 1 If there are additional Trusted Certificates to be added to the Certification Repository, repeat steps 1 - 2, otherwise click the Update Repository button to complete Trusted Certificate / CRL installation.



Before clicking the **Activate Certificate** button ensure that all CRLs have also been added to the Certification Repository.

When the **Activate Certificate** button is clicked, all added Trusted Certificates and CRLs are installed and the Collaboration Server displays a disconnection confirmation dialog box.



- 2 Click OK.
- 3 Login to the Collaboration Server to proceed with further management tasks.

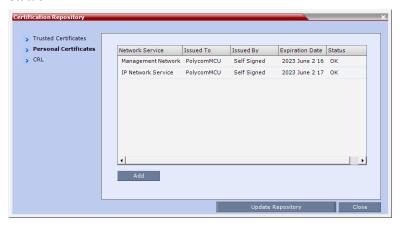
Trusted Certificates added to the Certification Repository are not automatically activated. They remain in the Trusted Certificates List until the **Activate Certificate** button is clicked, at which time all Trusted Certificates in the list are activated simultaneously.

Personal Certificates

Default Management and Default IP Network Service certificates can be viewed in the **Personal Certificates** dialog box.

They are listed alongside the service to which they are attached. By clicking the column headers the Trusted Certificates can be sorted by:

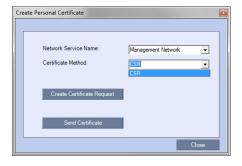
- Network Service
- Issued To
- Issued By
- Expiration Date
- Status



To add a Personal Certificate to the Certificate Repository:

- 1 In the Certification Repository Personal Certificates dialog box select the Network Service.
- 2 Click the Add button.

The **Add** dialog box is displayed with the configured parameters of the selected **Network Service** filled in.



- 3 Select the Certificate Method. (Default is CSR)
 - Only CSR can be selected for the Default Management Network Service.
 - > CSR or PFX/PEM can be selected for IP Network Services.

- 4 Optional. If **CSR** was selected as the Certificate Method:
 - a Click Create Certificate Request.

The Create Certificate Request dialog box is displayed with the Common Name field filled in.

b Complete the **Certificate Request** fields.

The two additional fields are defined as:

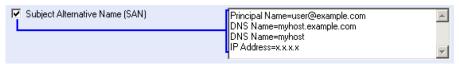
- Subject Alternative Name (SAN) This field is required when using EAP-TLS in conjunction with a Network Policy Server (MS-NPS). It allows the optional inclusion of:
 - Principle Name
 - DNS Name:

Long - FQDN

Short - Host only

- IP Address (IPv4 and IPv6)

When the **Subject Alternative Name** (**SAN**) check box is selected the input box becomes active, allowing the user to modify the example values provided, to match local certificate requirements and delete those that are not applicable.



The user can add up to 20 different SANs. If an incorrect SAN type is entered, an error message, Unsupported SAN type, is displayed when the **Send Details** button is clicked.



The **SAN** field option - DNS Name (FQDN) is not used for Machine Account validation. For example, the DMA will not validate the Collaboration Server unless the FQDN field in the **User Properties** dialog box is correctly filled in.

- Hash Method Select the output value for the Secure Hash Algorithm:
 - SHA-256 the output value is 256 bits.
 - SHA-1 the output value is 160 bits.

For backward compatibility, with previous versions, either SHA-1 or SHA-256 can be selected as the hash algorithm used in the creation of CSRs (Certificate Signing Requests).

5 Click Send Certificate.

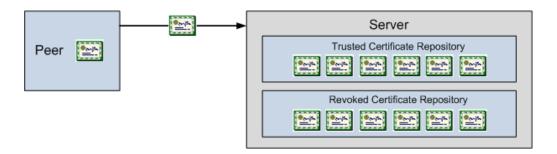
For all certificates, both Management and SIP TLS:

- Once the certificate is sent a message is displayed indicating successful installation of the certificate and the new certificate replaces the old certificate.
- If the certificate installation fails the old certificate continues to function and a message is displayed indicating one of the following the reasons for the failure:
 - Invalid password.
 - Certificate expired.
 - Certificate DNS name does not match Collaboration Server (service) DNS name.
 - Chain is not trusted

General - <Error message from the SSL library>.

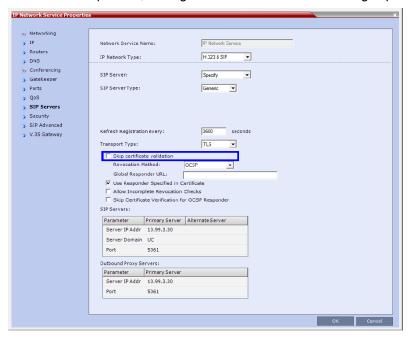
Certificate Validation

The credentials of each certificate received from a networked peer are verified against a repository of trusted certificates. Each networked entity contains a repository of trusted certificates. The digital signature of the certificate's issuing authority is checked along with the certificate's expiration date.



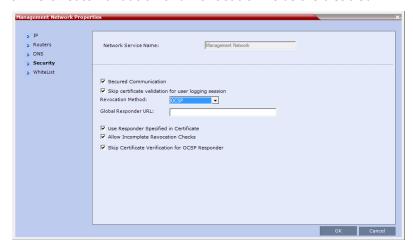
Validation of peer SIP TLS certificates against one or several installed CA certificates can be enabled or disabled for the Default Management and each defined IP Service by selecting or clearing the **Skip** certificate validation check box.

The check box is checked by default to **Skip certificate validation for user logging session** and no validation of expiration, CA signature or CRL/OCSP checking is performed.



Clearing the check box enables full validation requires that there be at least one CA certificate in the certificate repository, failing which a message *At least one CA certificate should be installed* is displayed.

If the **Secured Communication** option is unchecked in the **Management Network - Security** dialog box all **Certificate Validation** and **Revocation** fields are disabled.

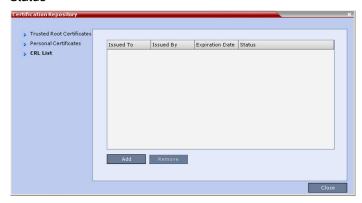


CRL (Certificate Revocation List)

A CRL contains a summary of the installed Certificate Revocation Lists.

By clicking the column headers the Certificate Revocation List can be sorted by:

- Issued To
- Issued By
- Expiration Date
- Status



If the CRL List is not valid for any reason an Active Alarm is created and a message is displayed. The Collaboration Server Web Client/RMX Manager connection to the Collaboration Server is not disabled.

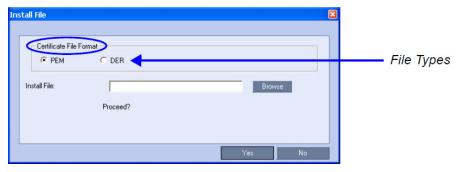
Adding a CRL

To add a CRL to the repository:

Repeat steps 1 - 5 for each CRL that is to be added to the Certification Repository.

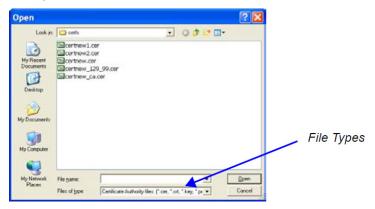
1 In the CRL List dialog box, click the Add button.

The Install File dialog box is displayed.



- 2 Select the Certificate File Format: PEM or DER.
- 3 Enter the certificate file name in the **Install File** field or click the **Browse** button.

The **Open** file dialog box is displayed. The files are filtered according to the file type selected in **Step b**.



- 4 Enter the Certificate file name in the **File name** field or click to select the certificate file entry in the
- 5 Click the Open button.

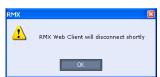
The certificate is added to the CRL List in the Certification Repository.

If there are additional CRLs to be added to the Certification Repository, repeat steps 1 - 5, otherwise click the **Activate Certificate** button to complete CRL / Trusted Certificate installation.



Before clicking the **Activate Certificate** button ensure that all Trusted Certificates have also been added to the Certification Repository.

When the Activate Certificate button is clicked, all added Trusted Certificates and CRLs are installed and the Collaboration Server displays a disconnection confirmation dialog box.



- 6 Click the **OK** button.
- 7 Login to the Collaboration Server to proceed with further management tasks CRLs added to the Certification Repository are not automatically activated. They remain in the CRL List until the **Activate Certificate** button is clicked, at which time all CRLs in the list are activated simultaneously.

Removing a CRL

To remove a CRL:

- 1 In the certificate list, select the CRL List to be removed.
- 2 Click the Remove button.

The certificate is removed and the Collaboration Server displays a disconnection confirmation dialog box.

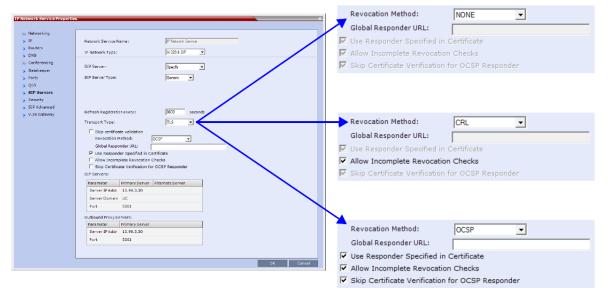


3 Click the **OK** button.

Login to the Collaboration Server to proceed with further management tasks.

Certificate Revocation

Certificate Revocation of IP Network and peer SIP TLS certificates for each defined IP Service can be enabled, disabled and configured:



Revocation Method

One of three Certificate Revocation Methods can be selected:

- NONE (Default) Certificate Revocation is not implemented.
- CRL Requires at least one CRL file be installed, failing which an error message, At least one CRL should be installed, is displayed.
- OCSP When selected, additional configuration options are displayed.

> Global Responder URL

- The format of the URL is validated and must be of the format: http(s)://responder.example.com/ocsp
- ♦ The URL can be either http or https.
- ♦ If the Global Responder URL does not respond an Active Alarm is raised.

Use Responder Specified in Certificate

- ♦ The default for this check box is unchecked.
- ♦ If the check box is checked Responder URL is taken from the certificate. If the certificate does not contain a Responder URL, the Global Responder URL is used.
- If the check box is unchecked the Global Responder URL is used. If the Global Responder URL is incorrectly configured a message, Global responder URL must be configured, is displayed.
- Allow Incomplete Revocation Checks

If OCSP is selected:

- ♦ If the check box is checked and the **Global Responder** or the **Responder Specified in the Certificate** does not respond for any reason the certificate is not considered revoked.
- ♦ If the check box is unchecked and the Global Responder or the Responder Specified in the Certificate does not respond for any reason the certificate is considered revoked.

If CRL is selected:

- ♦ If the check box is checked and the CRL of the specific CA is not loaded, all Certificates are the CA are not considered revoked.
- If the check box is unchecked and the CRL of the specific CA is not loaded, all Certificates are the CA are considered revoked.
- Skip Certificate Validation for OSCP Responder
 - ♦ No Certificate Validation is performed.
- System Flag:

Should intermittent login problems occur when logging in to the Collaboration Server's Management Network, the OCSP_RESPONDER_TIMEOUT system flag can be manually added to system.cfg and its value set to the number of seconds the Collaboration Server is to wait for an OCSP response from the OCSP Responder before failing the connection.

Default: **3** (seconds) Range: **1-20** (seconds)

Self-signed Certificate

In compliance with UC APL requirements, PKI Self-signed Certificates are supported for the both the Default Management and IP Network Services.

A mixture of Self-signed and CA-signed Certificates is supported, however a CA-signed certificate will always override a Self-signed Certificate.

Self-signed Certificate Creation

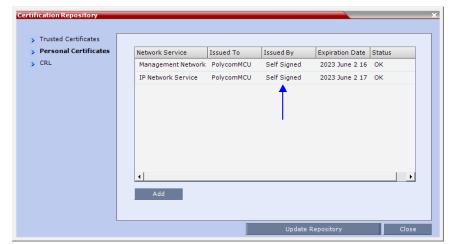
Self-signed Certificates are created during:

- Initial system start-up before any CA-signed Certificates have been installed.
- IP Network Services creation.
- Network Services updates that result in Host Name changes.
- Daily validity checks of Self-signed Certificates.
- Backup and Restore of the system configuration

Self-signed Certificate field values are automatically inserted when the certificate is created:

Self-signed Certificate Field Values - Creation

Field	Value
Signature Algorithm	SHA1
Issuer / Issued To	Service Host Name Both the Issuer and Issued To fields have the same values. CN = host name of the service name DC = Polycom OU = Self Signed Certificate O = Polycom MCU Note: The value of CN is derived from the IP Network Service Name, while the values of DC, OU and O are hard coded. For a full description of these fields see RFC 5280.
Valid from	Date of creation
Valid to	Date of creation + 10 years
Subject (Common Name)	Service Host Name
Public Key	2048 bits



Self-signed Certificates are indicated in the Certification Repository - Issued By field.

SIP TCP Keep-Alive

In compliance with UC APL requirements, the NAT Keep Alive method has been enhanced according to IETF RFC 5626 and For a full description of Keep Alive see IETF RFC 5626 and IETF RFC 6223.

Keep Alive behavior is defined for each IP Network Service and can be modified by adding the following system flags and modifying their values according to System Flags: SIP_TCP_KEEPALIVE_TYPE / BEHAVIOR . For more information see IP Network Services .

System Flags - SIP_TCP_KEEPALIVE_TYPE / BEHAVIOR

Flag	Possible Flag Values
SIP_TCP_KEEPALIVE_TYPE	NONE • No Keep Alive messages are sent.
	 MS (Default when Microsoft SIP Server Type is selected for the Network Service). Keep Alive messages are sent only after successful registration. A Pong response is not expected.
	RFC5626

- In the SIP Header, the Flow-Timer Header Field is mandatory.
- Keep Alive messages are sent only after successful registration. A Pong response is expected and if none is received, the value of the SIP_TCP_KEEP_ALIVE_BEHAVIOR system flag is checked.

If its value is:

DO_NOT_RE_REGISTRATION_WHEN_NO_PONG_RESPONSE

- ♣ For a Register Dialog, a Reregister Message is sent. There is no disconnection.
- ♣ For a Call Dialog, no further messages are sent. There is no disconnection.

If its value is: RE_REGISTRATION_WHEN_NO_PONG_RESPONSE

▲ Both Register and Call Dialogs are disconnected.

System Flags - SIP_TCP_KEEPALIVE_TYPE / BEHAVIOR

Flag	Possible Flag Values
SIP_TCP_KEEPALIVE_TYPE	 RFC6223 Behavior is the same as for RFC5626 with the following differences: ▲ In the SIP Header, the Via Header "keep" is mandatory. ▲ In the SIP Header, the Flow-Timer Header Field is optional.
	PLCM (Default when Generic SIP Server Type is selected for the Network Service). • For Call and successful Register Dialogues: ▲ Two CR LF character sequences are sent ▲ No PONG response is expected
SIP_TCP_KEEP_ALIVE_BEHAVIOR	If the value of the System Flag, SIP_TCP_KEEPALIVE_TYPE= RFC5626 or RFC6223 and no Pong is received, the value of this System Flag is checked. Possible Values: RE_REGISTRATION_WHEN_NO_PONG_RESPONSE DO_NOT_RE_REGISTRATION_WHEN_NO_PONG_RESPONSE (Default) For a full description see the description for the SIP_TCP_KEEPALIVE_TYPE flag (above).

Keep Alive Frequency

The Keep Alive frequency is set by the SIP Server using the Via Header keep and Flow Timer fields of the SIP Header.

If the Collaboration Server is functioning as the server, the Keep Alive frequency is set according to the hard coded values listed in the following table.

Keep Alive - Frequency

Field	Seconds
SIP_TCP_KEEPALIVE_DISABLE	None
SIP_TCP_KEEPALIVE_MS	300
SIP_TCP_KEEPALIVE_5626	60
SIP_TCP_KEEPALIVE_6223	
SIP_TCP_KEEPALIVE_PLCM	

User and Connection Management

Chairperson and Auditor user Authorization Levels are not supported in Ultra Secure Mode.

In Ultra Secure Mode (**ULTRA_SECURE_MODE=YES**), Users can be automatically disabled or locked out by the system when they do not log into the Collaboration Server application for a predefined period or if their login session does not meet Enhanced Security requirements. Users can be manually disabled by the administrator.

An administrator can enable a User who was disabled automatically by the system (in the Ultra Secure Mode) or manually by the administrator.

Additional security measures can be implemented in the Collaboration Server by setting the appropriate system flags. These measures control the system users, the user connections to the MCU and the user login process.

Managing system users includes:

- User types that are not supported when the Ultra Secure Mode is enabled.
- Disabling and enabling system Users.
- Renaming Users.
- Disabling inactive users.

Managing the user login process includes:

- Implementing Strong Passwords.
- Implementing password re-use / history rules.
- Defining password aging rules.
- Defining password change frequency.
- Forcing password change.
- Conference and Chairman Passwords.
- Locking out User.
- Displaying the User Login record.

Controlling the user sessions includes:

- Limiting the maximum number of concurrent user sessions.
- User session timeout.
- Limiting the maximum number of users that can connect to the system.

Managing the System Users

When the MCU is configured to Ultra Secure Mode (the **ULTRA_SECURE_MODE** is set to **YES**), the following user management rules are automatically enforced:

User Types

Auditor and chairperson user types are not supported.

 The SUPPORT user type is not allowed. If it exists, this user type is removed when the ULTRA_SECURE_MODE is set to YES and the system is restarted.

The Audit files can be retrieved by the Administrator User.

Disabling/Enabling Users

- An administrator can disable a user or enable a disabled user, including administrators.
- The last administrator cannot be disabled.

For more information see Disabling Inactive Users .

Renaming Users

- An administrator can rename any user, including administrators.
- A renamed user is considered by the system to be a new user and is forced to change his/her password.

Disabling Inactive Users

Users can be automatically disabled by the system when they do not log into the Collaboration Server application for a predefined period. When the Collaboration Server is configured to Ultra Secure Mode this option is enforced.

- To enable this option, the **DISABLE_INACTIVE_USER** system flag to a value between **1 to 90**. This value determines the number of consecutive days a user can be inactive before being disabled.
 - When flag value is set to **0** (default in standard security environment), this option is disabled.
 - The flag value is automatically set to 30 days when Ultra Secure Mode is enforced.
- The user is marked as disabled but is not deleted from the system administrator/operator database.
- The user remains disabled until re-enabled by an administrator.
- If a disabled user attempts to Login, an error message, Account is disabled, is displayed.
- The last remaining administrator cannot be disabled.

For more information see Disabling Inactive Users .

Managing the User Login Process

Implementing Strong Passwords

Strong Passwords can be implemented for logging into the Collaboration Server management applications. They can be implemented when the system is in standard security mode or when in **Ultra Secure Mode**.

The FORCE_STRONG_PASSWORD_POLICY System Flag, which enables or disables all password related flags cannot be set to NO and all Strong Passwords rules are automatically enabled and cannot be disabled when the ULTRA_SECURE_MODE System Flag is set to YES.

If an administrator modifies any of the **Strong Passwords** flag settings, all users are forced to perform the password change procedure, ensuring that all user passwords conform to the modified **Strong Passwords** settings.

Administrators can change passwords for users and other administrators. When changing passwords for him/herself, other administrators or other users, the administrator is required to enter his/her own administrator's password.

Strong Passwords rules are enforced according to the settings of the various **Strong Passwords** flags as described in System Flags affected by Ultra Secure Mode . Default settings of these flag change according to the system security mode.

Password Character Composition

- When the FORCE_STRONG_PASSWORD_POLICY System Flag is set to YES:
 - > A Strong Password must contain at least one of all of the following character types:
 - ♦ Upper case letters
 - ♦ Lower case letters
 - ♦ Numbers
 - ♦ Special characters: @ # \$ % ^ & * () _ = + | } { : " \] [; / ? > < , . (space) ~</p>
- When the FORCE_STRONG_PASSWORD_POLICY and ULTRA_SECURE_MODE System Flags are set to YES:
 - > A Strong Password must contain at least two of all of the following character types:
 - Upper case letters
 - ♦ Lower case letters
 - Numbers
 - Special characters: @ # \$ % ^ & * () _ = + | } { : " \] [; / ? > < , . (space) ~</p>
- Passwords cannot contain the User ID (User Name) in any form. Example: A user with a User ID,
 ben, is not permitted to use "123BeN321" as a password because BeN is similar to the User ID.
- Passwords cannot contain more than four digits in succession.

When the strong password option is enabled and the password does not meet the Strong Password requirements an error, **Password characteristics do not comply with Enhance Security requirements**, is displayed.

Password Length

The length of passwords is determined by the value of the MIN PASSWORD LENGTH System Flag.

- Possible flag values are between 0 and 20.
- A **System Flag** value of **0** means this rule is not enforced, however this rule cannot be disabled when the Collaboration Server is in **Ultra Secure Mode**.
- In **Ultra Secure Mode**, passwords must be at least 15 characters in length (default) and can be up to 20 characters in length.
- If the MIN_PASSWORD_LENGTH flag is enabled and the password does not meet the required length an error, Password is too short, is displayed.

If the minimum password length is increased, valid pre-existing passwords remain valid until users are forced to change their passwords.

Implementing Password Re-Use / History Rules

Users are prevented from re-using previous passwords by keeping a list of previous passwords. If a password is recorded in the list, it cannot be re-used. The list is cyclic, with the most recently recorded password causing the deletion of the oldest recorded password.

- The number of passwords that are recorded is determined by the value of the PASSWORD_HISTORY_SIZE System Flag. Possible values are between 0 and 16.
- A flag value of 0 means the rule is not enforced, however this rule cannot be disabled when the Collaboration Server is in Ultra Secure Mode.
- In Ultra Secure Mode, at least 10 passwords (default) and up to 16 passwords must be retained.

If the password does not meet this requirement, an error, New password was used recently, is displayed.

Defining Password Aging

The duration of password validity is determined by the value of the **PASSWORD_EXPIRATION_DAYS System Flag**.

- Passwords can be set to be valid for durations of between 0 and 90 days.
- If the System Flag is set to 0, user passwords do not expire. The System Flag cannot be set to 0
 when the Collaboration Server is in Ultra Secure Mode.
- In Ultra Secure Mode, the minimum duration can be set to 7 days and the default duration is 60 days.

The display of a warning to the user of the number of days until password expiration is determined by the value of the PASSWORD_EXPIRATION_WARNING_DAYS System Flag.

- Possible number of days to display expiry warnings is between 0 and 14.
- If the System Flag is set to 0, password expiry warnings are not displayed. The System Flag cannot be set to 0 when the Collaboration Server is in Ultra Secure Mode.
- In Ultra Secure Mode, the earliest warning can be displayed 14 days before passwords are due to expire and the latest warning can be displayed 7 days before passwords are due to expire (default setting).
- If a user attempts to log in after his/her password has expired, an error is displayed: User must change password.

Maximum Repeating Characters

There are two separate flags that control the maximum number of repeated characters permitted in a password, one for the user password and one for the chairperson (conference) password.

• MAX_PASSWORD_REPEATED_CHAR allows the administrator to configure the maximum number of consecutive repeating characters to be allowed in a user password.

Range: 1 - 4 Default: 2

 MAX_CONF_PASSWORD_REPEATED_DIGITS allows the administrator to configure the maximum number of consecutive repeating digits to be allowed in a conference password.

Range: 1 - 4 Default: 2

Defining Password Change Frequency

The frequency with which a user can change a password is determined by the value of the **MIN_PWD_CHANGE_FREQUENCY_IN_DAYS System Flag.** The value of the flag is the number of days that users must retain a password.

- Possible retention period is between 0 and 7 days. In **Ultra Secure Mode** the retention period is between 1 (default) and 7.
- If the **System Flag** is set to **0**, users do not have to change their passwords. The **System Flag** cannot be set to **0** when the Collaboration Server is in **Ultra Secure Mode**.
- If a user attempts to change a password within the time period specified by this flag, an error,
 Password change is not allowed before defined min time has passed, is displayed.

An administrator can assign a new password to a user at any time.

Forcing Password Change

When the system is in **Ultra Secure Mode** the user is forced to change his/her password as follows:

- After modifying the value of the **ULTRA_SECURE_MODE System Flag** to **YES**, all Collaboration Server users are forced to change their **Login** passwords.
- When an administrator creates a new user, the user is forced to change his/her password on first Login.
- If an administrator changes a users **User ID** name, that user is forced to change his/her password on his/her next **Login**.
- If a user logs in using his/her old or default password, the **Login** attempt will fail. An error, **User must change password**, is displayed.
- Changes made by the administrator to any of the **Strong Password** enforcement **System Flags** render users' passwords invalid.

Example: A user is logged in with a fifteen character password. The administrator changes the value of the MIN_PASSWORD_LENGTH System Flag to 20.

The next time the user tries to log in, he/she is forced to change his/her password to meet the updated **Strong Password** requirements.

Temporary User Lockout

When the ULTRA_SECURE_MODE System Flag is set to YES, Temporary User Lockout is implemented as a defense against Denial of Service Attacks or Brutal Attacks. Such attacks usually take the form of automated rapid Login attempts with the aim of gaining access to or rendering the target system (any network entity) unable to respond to users.

If a user tries to log in to the system and the **Login** is unsuccessful, the user's next **Login** attempt only receives a response from the Collaboration Server after 4 seconds.

User Lockout

User Lockout can be enabled to lock a user out of the system after three consecutive **Login** failures with same **User Name**. The user is disabled and only the administrator can enable the user within the system. User Lockout is enabled when the **USER_LOCKOUT System Flag** is set to **YES**.

If the user tries to login while the account is locked, an error message, Account is disabled, is displayed.

User Lockout is an Audit Event.

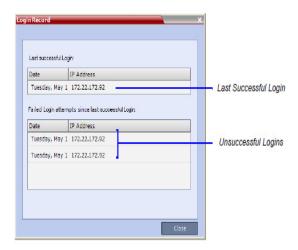
A system reset does not reset the **Login** attempts counter.

The time period during which the three consecutive **Login** failures occur is determined by the value of the **USER_LOCKOUT_WINDOW_IN_MINUTES System Flag**. A flag value of **0** means that three consecutive **Login** failures in any time period will result in **User Lockout**. Value can be between 0 and 45000.

The duration of the **Lockout** of the user is determined by the value of the **USER_LOCKOUT_DURATION_IN_MINUTES System Flag**. A flag value of **0** means permanent **User Lockout** until the administrator re-enables the user within the system. Value can be between 0 and 480.

User Login Record

The system can display a record of the last **Login** of the user. It is displayed in the **Main Screen** of the *Collaboration Server* **Web Client** or *Collaboration Server* **Manager**. The user **Login Record** display is enabled when the **LAST_LOGIN_ATTEMPTS System Flag** is set to **YES**.



Both lists display the:

- Date and Time of the Login attempt.
- IP Address of the workstation initiating the Login attempt.

The list of unsuccessful **Logins** can contain up to ten records.

Failed **Login** attempts are written to the system **Log Files** and are recorded as **Audit Events**. The **Audit** files can be retrieved by the Administrator User.

Controlling User Sessions

Management Sessions per System

It is possible for a several users to simultaneously log in to the Collaboration Server and initiate management sessions from different instances of the *Collaboration Server* **Web Client** or *Collaboration Server* **Manager** that are running on a single or several workstations.

The maximum number of concurrent management sessions (http and https connections) per system is determined by the value of the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_SYSTEM System Flag.

Any attempt to exceed the maximum number of management sessions per system results in the display of an error message: **Maximum number of permitted user connections has been exceeded. New connection is denied**.

The log in attempt is recorded as an **Audit Event**.

Sessions per User

It is possible for a user to log in to the Collaboration Server and initiate multiple management sessions from different instances of the **Collaboration Server Web Client** or **Collaboration Server Manager** that are running on a single or several workstations.

The maximum number of concurrent management sessions per user (http and https connections) is determined by the value of the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER System Flag.

Any attempt to exceed the maximum number of management sessions per user results in the display of an error message: A user with this name is already logged into the system. Additional connection is denied.

The log in attempt is recorded as an Audit Event.

Connection Timeout

If the connection is idle for longer than the number of seconds specified by the setting of the **APACHE_KEEP_ALIVE_TIMEOUT System Flag**, the connection to the Collaboration Server is terminated.

Session Timeout

If there is no input from the user or if the connection is idle for longer than the number of minutes specified by the setting of the **SESSION_TIMOUT_IN_MINUTES System Flag**, the connection to the MCU is terminated.

A flag value of **0** means **Session Timeout** is disabled, however this feature cannot be disabled when the MCU is in **Ultra Secure Mode**.

Erase Session History After Logout

In Ultra Secure Mode, the Collaboration Server Web Client and RMX Manager leave no session information on the user's workstation or the MCU after the user logs off.

Banner Display and Customization

The Login Screen and Main Screen of the Collaboration Server Web Client and the Collaboration Server Manager can display informative or warning text banners. These banners can include general information or they can be cautioning users to the terms and conditions under which they may log into and access the system, as required in many secured environments.

Banner display is enabled in the Setup > Customize Display Settings > Banners Configuration.

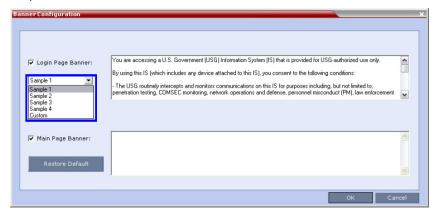


When the **ULTRA_SECURE_MODE** system flag is set to **YES**, the banners are displayed by default and cannot be disabled. When set to **NO** (default), banner display is according to the check box selection in the **Banners Configuration** dialog box.

The administrator can choose one of four alternative login banners to be displayed. The four alternative banners cannot be modified. A Custom banner (default) can also be defined.

The Main Page Banner is blank and can be defined.

The **Banner Configuration** dialog box allows the administrator to select a **Login Page Banner** from a drop-down menu.



One of the the following Login Page Banners can be selected:

- Non-Modifiable Banners
 - Sample 1
 - Sample 2
 - Sample 3
 - Sample 4
- Modifiable Banner
 - Custom (Default)

Guidelines for Customizing the Login Page Banner

- The Login Page Banner cannot be disabled when the Collaboration Server is in Ultra Secure Mode.
- The Login Page Banner must be acknowledged before the user is permitted to log in to the system.
- If a Custom banner has been created, and the user selects one of the alternative, non-modifiable banners the Custom banner not deleted.
- The Custom Login Page Banner banner may contain up to 1300 characters.
- An empty Login Page Banner is not allowed.
- Any attempt to modify a non-modifiable banner results in it automatically being copied to the Custom banner.

Non-Modifiable Banner Text

Sample 1 Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Sample 2 Banner

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users also may be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Sample 3 Banner

You are about to access a system that is intended for authorized users only. You should have no expectation of privacy in your use of this system. Use of this system constitutes consent to monitoring, retrieval, and disclosure of any information stored within the system for any purpose including criminal prosecution.

Sample 4 Banner

This computer system including all related equipment, network devices (specifically including Internet access), is provided only for authorized use. All computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized personnel and their entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information including personal information, placed on or sent over this system may be monitored. Use of this system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of any such unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

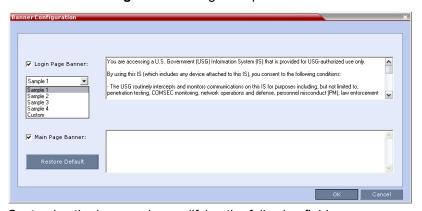
Customizing Banners

The **Login** and **Main Screen** banners can be customized to display conference information, assistance information or warning text as required in the **Ultra Secure Mode**.

To customize the banners:

1 In the Collaboration Server menu, click Setup > Customize Display Settings > Banners Configuration.

The **Banners Configuration** dialog box opens.



2 Customize the banners by modifying the following fields:

Banner Configuration

	Description		
Field	Check Box	Text Field	Restore Default Button
Login Page Banner	Select or clear the check box to enable or disable the display of the banner. Note: Banner display cannot be disabled in	Edit the text in this field to meet local requirements: Banner content is multilingual and uses Unicode, UTF-8 encoding. All text and special characters can be used. Maximum banner size is 100KB.	Click the button to restore the default text to the banner
Main Page Banner	when the ULTRA SECURE_MODE flag is set to YES.	The banner may not be left blank when the ULTRA SECURE_MODE flag is set to YES.	

3 Click the **OK** button.

Banner Display

Login Screen Banner

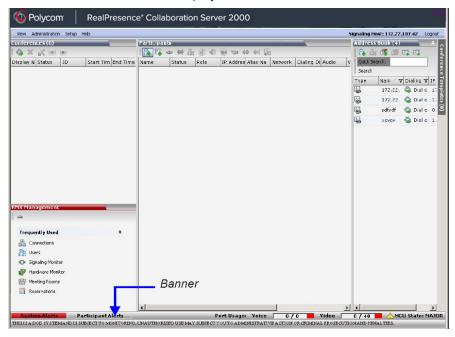
The **Login** screen banner can display any text, for example the terms and conditions for system usage. The default text is that required in **Ultra Secure Mode**. The user must acknowledge that the information was read and click the **Accept** button to proceed to the **Login** screen as shown in the following screen:



When the *Collaboration Server* is configured to work in **Ultra Secure Mode**, such as Maximum Security Environments, the display banner includes the terms and conditions for system usage as detailed in the default text: contained in **Sample Banner 1**.

Main Screen Banner

The Main Screen banner is displayed at the bottom of the screen, as follows:



When the *Collaboration Server* is configured to work in **Ultra Secure Mode**, such as the Maximum Security environment, the display banner includes the following default text:

THIS IS A DOD SYSTEM AND IS SUBJECT TO MONITORING, UNAUTHORIZED USE MAY SUBJECT YOU TO ADMINISTRATIVE ACTION OR CRIMINAL PROSECUTION AND PENALTIES.

Securing an External Database

TLS 1.0 is used when securing communications between the Collaboration Server and an external database. The certificate is installed on the database server and the Collaboration Server is the client. When the certificate is installed on the database server, all client requests and responses are transferred via secure port 443.

It is important to verify that the external database application is operating in secure mode before enabling secure external database communications on the Collaboration Server. The Collaboration Server checks the validity of external database's certificate before communicating. If there is a certificate error an **Active Alarm** is raised with **Error in external database certificate** in the description field.

To enable secure Collaboration Server Communications with an External Database:

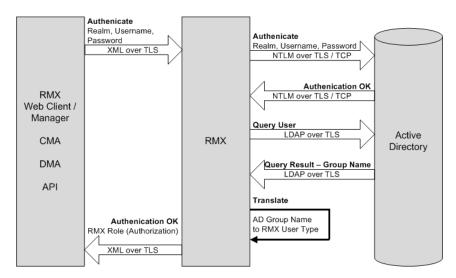
 Set the Collaboration Server to communicate with the database server via port 443 by setting the value of the System Flag EXTERNAL_DB_PORT in system.cfg to 443.

For more information see Modifying System Flags.

MS Active Directory Integration

It is possible to configure direct interaction between the Collaboration Server and **Microsoft Active Directory** for **Authentication** and **Authorization** of **Management Network** users.

The following diagram shows a typical user authentication sequence between a **User**, Collaboration Server and **Active Directory**.



Directory and Database Options

Ultra Secure Mode

Internal Collaboration Server database and Active Directory

Authentication is first attempted using the internal Collaboration Server database. If it is not successful authentication is attempted using the **Active Directory**.

Standard Security Mode

Internal Collaboration Server database + External Database

First authentication is via the internal Collaboration Server database. If it is not successful, authentication is via the **External Database**.

Internal Collaboration Server database + External Database + Active Directory

- Management Logins
 - First authentication is via the internal Collaboration Server database. If it is not successful, authentication is via the **Active Directory**.
- Conference Queries (Chairperson Password, Numerical ID etc.)
 - First authentication is via the internal Collaboration Server database. If it is not successful, authentication is via the **External Database**.

Guidelines

- The Collaboration Server maintains a local record of:
 - > Audit Events users that generate these events are marked as being either internal or external.
 - Successful user logins
 - > Failed user login attempts
- User passwords and user lockout policy for external users are managed via Active Directory's integration with the user's host machine.
- Enabling or disabling Active Directory integration does not require a reset.
- In Standard Security Mode multiple accounts of all user types are supported. In Ultra Secure Mode, enabling Active Directory integration is only permitted if the Collaboration Server only has one local Administrator User.
- Multiple Machine Accounts with various roles are supported.
- Microsoft Active Directory is the only directory service supported.
- Active Directory integration is configured as part of the Management Network.
- Both IPv4 and IPv6 addressing are supported.
- In Standard Security Mode, the Active Directory can be queried using NTLM with or without TLS
 encryption. In Ultra Secure Mode, TLS encryption is required.
- Server and client certificate validation requests use LDAP with or without TLS encryption.



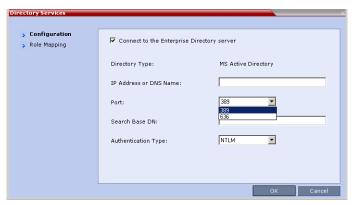
- When using *LDAP* over *TLS*, in addition to using port **389** with *STARTTLS*, the administrator has the option of using port **636**.
- The Active Directory setting define Send NTLMv2 response only. Refuse LM & NTLM (in the group policy management -> forest -> polycomdemo.com -> group policy objects -> default domain policy -> edit ->computer configuration -> policies -> windows settings -> local policies -> security options -> network security:Lan Manager authentication level) is not supported with the Collaboration Server.

Enabling Active Directory Integration

To configure Directory Services:

1 On the Collaboration Server Menu, click Setup > Directory Services.

The **Directory Services** - **Configuration** dialog box is displayed.

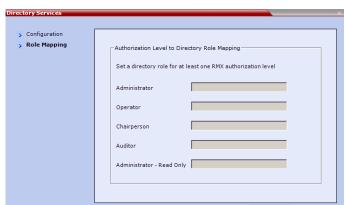


2 Modify the following fields.

Directory Services - Configuration

Field	Description
Connect to the Enterprise Directory Server	Select this check box to enable or disable the Active Directory feature.
IP Address or DNS Name	Enter the IP address or DNS name of the Enterprise Directory Server (Active Directory).
Port	Select the <i>Port</i> according to the <i>Authentication Protocol</i> to be used: • 389 - <i>NTLM</i> over <i>TCP</i> • 636 - <i>NTLM</i> over <i>TLS</i>
Search Base DN	Enter the starting point when searching for <i>User</i> and <i>Group</i> information in the <i>Active Directory</i> . For example if the <i>Domain Name</i> is: mainoffice.bigcorp.com.uk The entry in this field should be: CN=Users, DC=mainoffice, DC=bigcorp, DC=come, DC=uk
Authentication Type	Only NTLM can be used.

3 Click the Role Mapping tab.



The **Directory Services** - **Role Mapping** dialog box is displayed.

Each of the Collaboration Server user types: **Administrator**, Administrator Read-Only, **Auditor**, **Operator** and **Chairperson** can be mapped to only one **Active Directory Group** or **Role** according to the customer's specific implementation.

- > In Ultra Secure Mode there are only two user types: Operator and Administrator.
- A Collaboration Server user that belongs to multiple **Active Directory Groups** is assigned to the **Group** with the least privileges.
- 4 Map the Collaboration Server User Types, to their Active Directory roles by modifying the following fields.

Directory Services - Role Mapping

Field	Description
Administrator	At least one of these <i>User Types</i> must be mapped to an <i>Active</i>
Administrator Read-Only	Directory Role.
Operator	
Chairperson	
Auditor	

5 Click OK.

Restoring the RealPresence® Collaboration Server (RMX®) 1500/2000/4000 Using the USB Port

When the RMX is in **Ultra Secure Mode**, the **Restoring the RealPresence® Collaboration Server Using the USB Port** procedure can be used to set the RMX back to its factory default settings, if for any combination of factors the system becomes unstable or unmanageable.

For a full description of this procedure see the *Polycom® RealPresence® Collaboration Server (RMX®)* 1500/2000/4000 Deployment Guide for Maximum Security Environments, Restoring the RMX Using the USB Port .

MLPP (Multi Level Precedence and Preemption)

In compliance with **UC APL** requirements, **Quality of Service** (**QoS**) can be more accurately modified to suit local needs with the addition of **Multi Level Precedence** and **Preemption** methods for call prioritizing and call handling.

QoS is important when transmitting high bandwidth audio and video information. **QoS** can be measured and guaranteed in terms of:

- Latency
- Low packet throughput
- Average delay between packets
- Jitter (variation in delay)
- Transmission error rate
- Order of packet delivery

Precedence is the method by which a call is assigned a priority level. The **RMX** supports two separately defined and configurable **Domains**, each having its own **Precedence** policy.

For a full description of Precedence see IETF RFC 2474.

One of the following **Precedence Levels** is assigned to all calls:

Precedence Levels

Highest Priority	FLASH-OVERRIDE-OVERRIDE (Classified Networks only)
	FLASH-OVERRIDE
	FLASH
	IMMEDIATE
	PRIORITY
Lowest Priority	ROUTINE

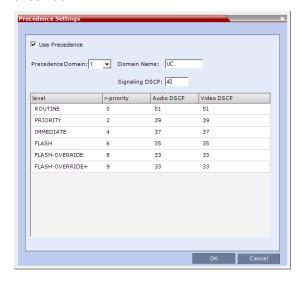
Conferences can have a mix of participants from different **Precedence** domains and network domains.

Precedence is supported for both IPv4 and IPv6.

Preemption is the method whereby, when system resources are insufficient, lower priority calls are terminated and their resources assigned to higher priority calls. **Preemption** is typically a function of network components such as the **Local Session Controller (LSC)**. To the **RMX**, a preempted call appears as a disconnected call.

Enabling Precedence

Precedence is disabled by default. It is enabled by using the **Setup > Precedence Settings** menu to display the **Precedence Settings** dialog box. **Precedence** is enabled by selecting the **Use Precedence** check box.



See Configuring and Modifying Precedence Domains and DSCP Values .

When **Precedence** is enabled, all other **QoS** system settings are overridden by the parameters sent in the **SIP Message**. For more information about **QoS**, see the *RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 Administrator's Guide Modifying the Default IP Network Service.

SIP Message

A **SIP Message** is a request or a response between network entities that communicate using the SIP protocol. The **SIP Message** header contains **Precedence** and **Resource Priority** (**r-value**) information and an optional **Require** tag for each call.

For a full description of SIP Messages see IETF RFC 3261.

For a full description of Resource Priority (DSCP) see IETF RFC 2474.

For a full description of SIP r-priority see IETF RFC 4412.

Dial-in calls

If the Use Precedence check box in Precedence Settings is selected:

 The RMX uses the information in the SIP Message header to match the call to a Precedence Domain and a Precedence Level. Table 5-45 summarizes of the default values.

Precedence Domain and Resource Priority - DSCP Default Values

Resource Priority	Precedence Level		DSCP Value	
		Audio	Video	
9	FLASH-OVERRIDE-OVERRIDE	33 (0x21)	33 (0x21)	

Precedence Domain and Resource Priority - DSCP Default Values

Resource	Precedence Level		DSCP Value	
Priority		Audio	Video	
8	FLASH-OVERRIDE	33 (0x21)	33 (0x21)	
6	FLASH	35 (0x23)	35 (0x23)	
4	IMMEDIATE	37 (0x25)	37 (0x25)	
2	PRIORITY	39 (0x27)	39 (0x27)	
0	ROUTINE	51 (0x33)	51 (0x33)	
NONE	No Resource Priority header for backward co	ompatibility		

- SIP Dial in participants, both defined and undefined, do not inherit Precedence or Domain
 characteristics from the Participant's Address Book. (Additional fields, added to the Participant's
 Properties Advanced and Address Book Advanced dialog boxes are used to enter and modify
 Precedence or Domain characteristics for SIP Dial-out participants.)
- Incoming calls are accepted or rejected depending on the:
 - ➤ Value of the REJECT_INCORRECT_PRECEDENCE_DOMAIN_NAME System Flag.
 - Match or mismatch of the Precedence Domains, set in the RMX and contained in the incoming SIP Message r-value.
 - ♦ The r-value is of the following format:

r-value = <domain name>-<subdomain>.<r-priority>

Table 5-46 shows an example of calls accepted or rejected assuming:

- Domain Name = UC
- > Sub Domain = 000000
- > r-priority = 2

Example - Call Acceptance by System Flag Value and Precedence Domain Matching

Call Acceptance			
Precede	ence Domain	Flag Value: REJECT_INCORRECT_PREC	EDENCE_DOMAIN_NAME
RMX	Incoming SIP Message	YES	NO (Default)
UC	UC		
UC	UC.00001	_	
UC	UC.00002	Call Assented	
UC-00000	UC-00000	- Call Accepted	Call Accepted
UC-00000	UC-00001	_	and
UC-00000	UC	_	assigned ROUTINE priority
UC	UC00002		
UC	UCC	Call Rejected	
UCC	UC	_	

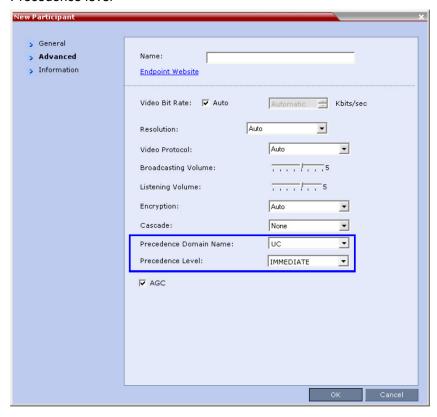
- Rejected calls receive a 417 Error response.
- If the Require tag is null, the call is connected and assigned ROUTINE priority in the first defined Precedence Domain
- If the **Use Precedence** check box in **Precedence Settings** is cleared, the RMX will not reject such calls. The LSC is responsible for rejecting such calls.

Dial-out calls

For **Dial-out** calls, the **SIP Message** header information for the **Precedence Domain** and **Resource Priority** (**r-priority**) of the call is configurable.

Additional fields in the **Participant's Properties - Advanced** and **Participant's Address Book - Advanced** dialog box are used to modify these parameters:

- Precedence Domain Name
- Precedence level



Precedence Level Change

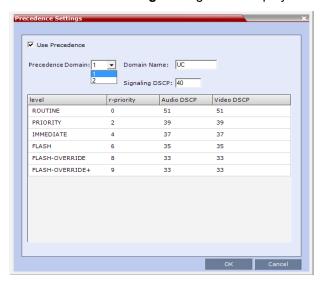
The **Precedence Level** of all calls can only be changed by the **LSC** sending a **Re-Invite** or similar **SIP Message** to the Collaboration Server.

Configuring and Modifying Precedence Domains and DSCP Values

The **Precedence Domains** and **DSCP** values for each **Precedence Domain** can be configured and modified per **MCU**.

To configure Precedence Settings:

On the RMX menu, click Setup > Precedence Settings
 The Precedence Settings dialog box is displayed.



2 Optional: Modify the values if required.

Precedence Settings - Domains, Levels and DSCP Values

Field	Description
Use Precedence	Select or clear the check box to enable or disable <i>Precedence</i> . Default: Cleared (<i>Precedence</i> disabled)
Precedence Domain	Select the <i>Precedence Domain</i> to be modified, 1 or 2, from the drop-down menu. Possible Values: 1 / 2
Domain Name	Enter the required <i>Domain Name</i> .
Signaling DSCP	Modify the <i>DSCP</i> value of the <i>Signaling DSCP</i> . A single <i>Signaling Proxy</i> is used for all <i>Precedence Levels</i> . Default: 40 Range: 0 - 63

Precedence Settings - Domains, Levels and DSCP Values

Field	Description
Level	 r-priority, Audio DSCP and Video DSCP values can be modified for each of the six Precedence Levels: ROUTINE PRIORITY IMMEDIATE FLASH FLASH-OVERRIDE FLASH-OVERRIDE+
r-priority	Modify the <i>r-priority</i> value for the <i>Level</i> . Range: 0 - 255. Default: ROUTINE - 0, PRIORITY - 2, IMMEDIATE - 4, FLASH - 6, FLASH-OVERRIDE - 8, FLASH-OVERRIDE+ - 9
Audio/Video DSCP	Modify the <i>DSCP</i> value for the <i>Audio/Video DSCP</i> . Range: 0 - 63. Default: ROUTINE - 51, PRIORITY - 39, IMMEDIATE - 37, FLASH - 35, FLASH-OVERRIDE - 33, FLASH-OVERRIDE+ - 31

3 Click OK.

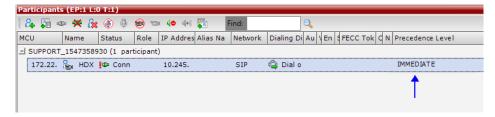
System Flags

The following **System Flags** must be added to **system.cfg** if their values are to be modified:

- QOS_MANAGEMENT_NETWORK the overall hex value of the DiffServ field (not just the value of the DSCP portion) is used as the DSCP value for the RMX Management Network.
 - > **Default**: 0x10
 - > Range: 0x00 0xFC
- REJECT_INCORRECT_PRECEDENCE_DOMAIN_NAME see Dial-in calls (above) for a
 description of this flag.
 - Default: NO
 - > Range: YES / NO

Monitoring Precedence Level

The Precedence Level of each connected participant is listed in the Participants list pane.



IEEE 802.1X Authentication

In compliance with **UC APL** requirements for enhanced security of wireless local area networks that follow the **IEEE 802.11** standard, support for **802.1X Authentication** has been included in this version.

802.1X Authentication requires that the **RMX** registers with a **802.1X Authentication Server and** is supported on **RMX 1500/2000/4000** The authentication protocol is applied to each the following **Network Interface Controllers (NICs)**:

- Management
- Signaling
- Media



- For RMX 2000, Network Separation must be implemented before configuring 802.1X
 Authentication.
- 802.1X Authentication is not supported in Microsoft environments.

The following 802.1X Authentication methods are supported:

- EAP-MD5
- EAP-TLS
- PEAPv0
- MSCHAPv2

Certificate Repository

Implementation of **802.1X Authentication** requires a certificate, which is obtained from the **Certificate Repository**.

- Either one TLS certificate is retrieved for all IP services and their associated NICs.
 - If one certificate is retrieved for all NICs, the RMX will use the Management Certificate for all the NICs.

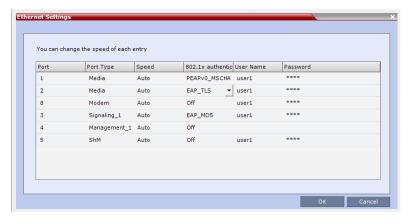
or

- A TLS certificate for each IP service and their associated NICs is retrieved from the Certificate Repository:
 - ➤ If several different **TLS** certificates are retrieved, each **NIC** will use the certificate of the service that it is associated with.
 - ♦ In a system configured with Multiple Network Services each IP service will use its own certificate.
 - ♦ A NIC that does not have its own certificate will first attempt to use the Management Certificate before using a self-signed certificate.

Enabling and Configuring 802.1X Authentication

802.1X Authentication for each **NIC** is enabled or disabled in the **Setup > Ethernet Settings** dialog box. The following additional table columns are used to modify these parameters:

- 802.1X Authentication
- User Name
- Password

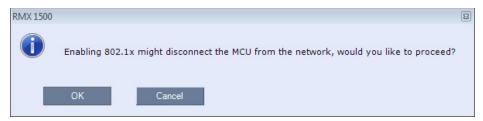


Modify the **Ethernet Settings** table fields as set out below:

802.1X Authentication - Configuration

Field	Description
802.1x Authentication	For each <i>NIC</i> , click the arrow to open the drop-down menu and select (or disable) the <i>802.1X Authentication</i> method: Off EAP-MD5 EAP-TLS PEAPv0 MSCHAPv2
User Name	Enter the <i>User</i> name that the RMX will use to register with the <i>802.1X</i> Authentication Server. This must be the RMX's <i>DNS</i> name and can be up to 256 characters. Note: If the <i>Domain Name (DC)</i> field was completed in the <i>Certificate Request</i> , the <i>User</i> must be: <common (dns)="" name="">@<domain (dc)="" name=""> as set out in the <i>Certificate Request</i>.</domain></common>
Password (EAP-MD5, PEAPv0 and MSCHAPv2 only)	Enter the <i>Password</i> , that the RMX will use to register with the <i>802.1X</i> Authentication Server. Up to 256 Unicode characters can be used. The <i>Password</i> is always displayed as four asterisks.

Enabling **802.1X Authentication** can result in the RMX being disconnected from the network and a warning message is displayed:



System Flags

The following system flags are used to manage the **802.1X Authentication** process. They must be manually added to **system.cfg** if their default values need to be modified.

802.1X Authentication System Flags

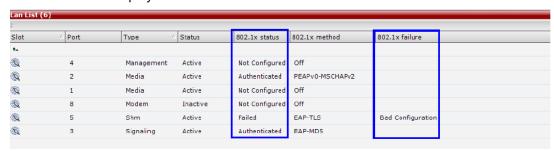
Flag name	Description
802_1X_CERTIFICATE_MODE	Determines whether one <i>TLS</i> certificate is retrieved from the <i>Certificate Repository</i> for all <i>IP</i> services or if multiple certificates will be retrieved, one for each <i>IP</i> service. Range: ONE_CERTIFICATE, MULTIPLE_CERTIFICATE Default: ONE_CERTIFICATE.
802_1X_SKIP_CERTIFICATE_VALIDATI ON	 If the flag value is: YES - The retrieved certificate is not validated against the CA certificate. NO - The retrieved certificate is validated against the CA certificate. Validation failure raises an Active Alarm and is reported in the Ethernet Monitoring dialog box. Range: YES, NO. Default: YES.
802_1X_CRL_MODE	 If the flag value is: ENABLED - Forces CRL checking. The system fails the connection request if the certificate has been revoked or if there is no CRL. OPTIONAL - The system fails the connection request if the certificate is revoked but does not fail the connection request if there is no CRL. DISABLED - Does not check the CRL and does not fail the connection request based on the CRL content. Range: ENABLED, OPTIONAL, DISABLED Default: DISABLED.
802_FIPS_MODE	If the flag value is YES, the availability of the MD5 Authentication Protocol will neither be displayed as selectable option nor supported. Range: YES/NO. Default: NO

Disabling 802.1X Authentication

Switching to http mode from https mode by inserting a USB key containing a file named RestoreFactorySecurityDefaults.txt into the RTM-IP USB port disables 802.1X functionality

Ethernet Monitoring

802.1x Status is displayed in the Hardware Monitor - LAN List.



The following 802.1X Statuses are possible:

- Authenticated
- Not Configured
- Failed

The following 802.1X Failure reasons are possible:

- Bad Configuration
- Link Status not Detected

White List Access

In compliance with **UC APL** requirements for enhanced security of web access to the RMX, a **White List** containing the addresses of IP Networking Entities permitted to connect to the **RMX's Management Network** is implemented - **Networking Entities** such as **Network Hosts**, **Control Workstations**, **Gatekeepers SIP/ DNS Servers**, etc.

Guidelines

- Only administrators can access and modify the White List.
- During First Time Installation and Configuration, when enabling the White List, the IP address of the workstation used to run the RMX Web Client is automatically added to the White List.
- The last White List entry cannot be deleted to prevent lock out. Any attempt to enable an empty White
 List results in the display of an error message: WhiteList is empty please add IP's to the list if you
 want to enable WhiteList.
- Both IPv4 and IPv6 are supported.
- Web access to the RMX for http and https is through ports 80 and 443 respectively.
- The White List can hold up to 100 entries. An error message is displayed when exceeding this limit.
- Access is blocked at the firewall for devices with IP addresses not listed in the White List.
- The White List is saved during Backup, Restore and Upgrade processes.

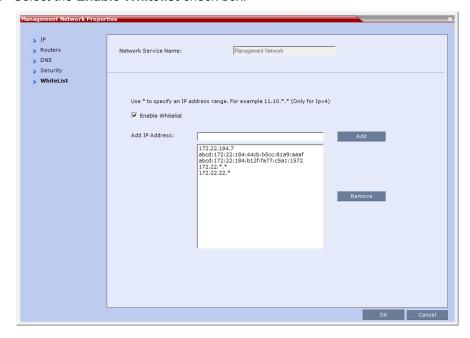
- Changes to the White List are written to the Auditor Event File.
- Alterations to the White List do not require a system reset.

Enabling, Disabling and Modifying the White List

The use of **White List** in the environment can be enabled or disabled in the **Management Network Service** - **White List** dialog box.

To enable, disable, view or modify the White List:

- 1 In the RMX Management pane, click the IP Network Services.
 - The IP Network Services pane is displayed.
- 2 In the IP Network Services list pane, double-click the Management Network entry.
 - The **Management Network** dialog box is displayed.
- 3 Click the WhiteList tab.
 - The WhiteList dialog box is displayed.
 - If there are no entries in the White List, it is disabled to prevent lock out.
 - If the White List is disabled none of the IP addresses in the list are displayed.
 - > The Add and Remove buttons are only active if the Enable Whitelist check box is selected.
- 4 Select the Enable Whitelist check box.



All **IP** addresses in the list are displayed and the **Add** and **Remove** buttons become active.

5 Modify the White List.

Both **IPv4** and **IPv6** addresses are supported and the system will only allow an entry of the type of **IP** addresses for which the **Management Network Service** is configured according to Table 5-51.

IP Address Modes

IP Address Modes		
RMX	Workstation / Device	
IPv4	IPv4	
IFV4	IPv4 & IPv6	
IPv6	IPv6	
IFVO	IPv4 & IPv6	
	IPv4	
IPv4 & IPv6	IPv6	
	IPv4 & IPv6	

- ▶ If the system changes its IP addressing mode (e.g. from IPv4 only to both IPv4 &6) while the White List is enabled, the White List is disabled and a message, White list has been disabled please reconfigure, is displayed.
- ➤ IPv4 addresses can be added as a range by using the wildcard character, *, to substitute the 3rd and 4th dotted decimal numbers of the IP address, e.g. 11.10.*.*
- a To Add IP addresses:

For each IP address to be added to the White List:

i) In the Add IP Address field enter an IP address to be added to the White List and click the Add button.

If an invalid **IP** address is entered, an error message is displayed and the administrator is prompted to enter a correct IP address.

If a duplicate **IP** address is entered, a message: **Duplicate IP's are not allowed in WhiteList** is displayed.

ii) When all the IP addresses have been added, click OK.

A message is displayed: Applying white list will limit RMX web access to the configured IP list, are you sure you want to continue?

- iii) Click Yes to apply the modified White List.
 - **b** To **Remove IP** addresses:

For each **IP** address to be removed from the **White List**:

- i) In the White List, click to select an IP address to be removed from the White List.
- ii) Click the **Remove** button.
- ii) When all the **IP** necessary addresses have been removed, click **OK**.

A message is displayed: Applying white list will limit RMX web access to the configured IP list, are you sure you want to continue?

iii) Click Yes to apply the modified White List.

Alternative Network Address Types (ANAT)

In compliance with UC_APL_NET_0007 Alternative Network Address Types (ANAT) is supported.

When the RMX is configured for IPv4 and IPv6 Addressing, the addition of the sdp-anat option tag in the SIP Require and SIP Supported headers allows a mixture of IPv4 and IPv6 addressing to be specified by the Session Description Protocol (SDP).

For a full description of ANAT see IETF RFCs 4091 and 4092.

Guidelines

- BFCP over TCP is not supported in Ultra Secure Mode. It's associated Content channel is not available.
- BFCP over UDP is supported in Ultra Secure Mode.
- If the RMX is configured for both IPv4 and IPv6, IPv4 addressing is given preference when establishing the connection.
- If an Outbound Proxy is configured, its transport type is used.
- If an Outbound Proxy is not configured, the SIP Server's (Registrar) transport type is used.

The **Outbound Proxy** and the **SIP Server** must be configured with one type only either according to the **IP** address type or according to the **DNS Resolution** type. However, if the RMX is configured for **IPv4&IPv6** then the **SIP Contact** field will contain both **IPv4** and **IPv6** addresses.

System Flag

The **ANAT Protocol** selection is controlled by the **ANAT_IP_PROTOCOL System Flag**. To modify it, manually add it to **system.cfg** and set its value as described in Table 5-52.

Range: DISABLED, AUTO, PREFER IPv4, PREFER IPv6

Default:

- ▶ If the ULTRA SECURE MODE System Flag is set to NO: DISABLED.
- If the ULTRA SECURE MODE System Flag is set to YES: AUTO.

ANAT_IP_PROTOCOL System Flag Values for Dial in Dial out

Value	Behavior - Dial in and Dial out
DISABLED	sdp-anat does not appear in SIP headers and the SDP does not contain a mixture of IPv4 and IPv6.
	If an endpoint requests ANAT (sends the Require: sdp-anat tag) the RMX will accept the call.
AUTO	sdp-anat appears in SIP headers.
	Dial in: The IP Version preference is according to the SDP priority.
	Dial out: IPv4 is advertised first.
PREFER_IPv4	sdp-anat appears in SIP headers.
	Dial in: IPv4 is the IP Version preference.
	Dial out: IPv4 is advertised first.

ANAT_IP_PROTOCOL System Flag Values for Dial in Dial out

Value	Behavior - Dial in and Dial out
PREFER_IPv6	sdp-anat appears in SIP headers. Dial in: IPv6 is the IP Version preference Dial out: IPv6 is advertised first.

BFCP Over UDP – AS-SIP Content

In compliance with UCR 2008 Change 3, AS-SIP (Assured Services-Session Initiation Protocol) Content flow is an implementation of SIP that utilizes SIP's built in security features.

When using **AS-SIP Content**, the **media line** of the content channel is not sent as part of the initial **SDP Offer/Answer** message sequence. The **media line** of the **Content** channel is only sent to the **MCU** when an endpoint wanting to share **Content** initiates **Content** sharing. The Collaboration Server (RMX) then sends the **Content media line** to all conference participants using an **SDP Re-invite**.

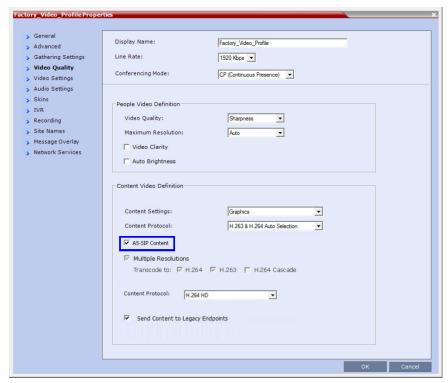
Guidelines

- AS-SIP Content is shared using Multiple Resolutions (Content Transcoding) and is not supported
 in any other Content sharing mode such as H.263 Content and H.264 Cascade and SVC
 Optimized Content Protocol.
- Multiple Resolutions consumes system video resources. If sufficient system video resources are
 not available, a conference with AS-SIP Content enabled in its Profile, will not be created. An error:
 Conference could not be created due to lack of Content DSP resources, is displayed.
- The SIP BFCP UDP application line is included in SDP Offer/Answer message sequence.
- An endpoint declaring SIP BFCP TCP is connected with video and audio but without Content. The SIP BFCP TCP channel will not be connected.
- The following resolutions are supported with H.264 HD Content protocol. Only when H.264 HD is selected, these resolutions are enabled for selection:
 - ➤ HD 720p5
 - ➤ HD 720p30
 - ➤ HD 1080p15
- Endpoints that do not support receiving H.264 Content at a resolution of HD 720p5 or greater are considered Legacy Endpoints and will receive Content using the people video channel.
- Endpoints that do not support transmitting H.264 Content at a resolution of HD 720p5 or greater are
 considered Legacy Endpoints and will transmit Content using the people video channel. Depending
 on the endpoint type, these endpoints may not be able to transmit Content at all this is dependent
 on the endpoint and is not controlled by the RMX.
- A mixture of older, non **AS-SIP** compliant and **AS-SIP** compliant endpoints are supported in the same conference and are able to share **Content**.
- An endpoint connecting during a Content session is immediately sent an SDP Re-invite that includes the connect media line and will receive Content.
- An endpoint connecting after Content started and was stopped will receive the SDP Re-invite and the content media line only after a new Content request is sent.

Once Content has been initiated by one of the endpoints, the Content channel will be opened to all
endpoints and remain open even if the Content sharing endpoint stops sharing Content.

Enabling AS-SIP Content

AS-SIP Content is enabled in the New Profile / Profile Properties - Video Quality tab.



When the **AS-SIP Content** check box is selected the following are automatically enabled and cannot be disabled:

- Send Content to Legacy Endpoints
- Multiple Resolutions

System Flag

The time that the **RMX** waits for endpoints to respond to its **SDP Re-invite** is determined by a timer. The timer duration, in seconds, is controlled by the **AS_SIP_CONTENT_TIMER System Flag**. Its default value is 10 seconds. To modify the timer value, manually add this flag to **system.cfg** and modifying its value as required:

Range: 1 - 60 seconds. (Values outside this range are rejected and an error message is displayed.)

Internet Control Message Protocol (ICMP)

ICMP (Internet Control Message Protocol) is used to send messages between networked entities. It is typically used to send and receive information concerning:

- Communications errors in network applications
- Remote host reachability and availability
- Network congestion (latency)
- Traffic redirection

Malicious devices can however use these capabilities in order to divert, intercept, detect, network traffic.

The following **System Flags** have been added to enable the administrator to control **ICMP Redirect** and **Destination Unreachable** messages:

- ENABLE_ACCEPTING_ICMP_REDIRECT
- ENABLE_SENDING_ICMP_DESTINATION_UNREACHABLE

By setting the value of these flags to NO the risk of malicious behavior can be mitigated.

For a full description of ICMP see RFC 792.

Guidelines

- Both flags apply to all MCU platforms: RealPresence Collaboration Server (RMX)
 1500/2000/4000/RealPresence Collaboration Server (RMX) 1800/RealPresence Collaboration
 Server 800s).
- Both flags apply to all Ethernet connections: Management, Signaling, Media, Modem. etc.

System Flag: ENABLE_ACCEPTING_ICMP_REDIRECT

This **System Flag** enables the administrator to control whether the RMX accepts or rejects **ICMP Redirect Messages (ICMP** message type #5), typically used to instruct routers to redirect network traffic through alternate network elements.

- Range: YES / NO
- Default:
 - > Ultra Secure Mode: NO Redirect messages or ignored.
 - Default Security Mode: YES Redirect messages are accepted.

System Flag: ENABLE_SENDING_ICMP_DESTINATION_UNREACHABLE

This **System Flag** enables the administrator to control whether the RMX sends **ICMP Destination Unreachable Messages (ICMP** message type #3).

Destination Unreachable Messages are sent when the RMX receives a **UDP** packet on a port configured for **TCP**, or receives a **UDP** packet on a port configured for TCP, or when, in real time, a packet is not processed in the prescribed time interval. For detailed timestamp information see **RFC 792**.

The **Destination Unreachable Message** may also be sent when **Network** or **Host** is unreachable (sent by the router) or the **Port** is unreachable (sent by the RMX).

• Range: YES / NO

- Default:
 - Ultra Secure Mode: NO Destination Unreachable Message is never sent.
 - Default Security Mode: YES Destination Unreachable Message is sent when needed.

Modifying the flag values

To modify the **System Flags** values, the flags must first be manually added to **system.cfg**. For more information about **System Flags**, see Manually Adding and Deleting System Flags.

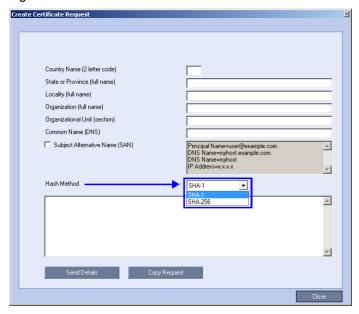
Password Encryption

In compliance with UC APL, FIPS 140-2 the SHA-256 (Secure Hash Algorithm) is applied to:

- Application login passwords.
- Linux operating system passwords.
- CSRs (Certificate Signing Requests).

The output value for SHA-256 is 256 bits whereas for SHA-1 the output value is 160 bits.

For backward compatibility with previous versions, either **SHA-1** or **SHA-256** can be selected as the hash algorithm used in the creation of **CSRs**.



Upgrade / Downgrade Guidelines

The RMX configuration, including users and passwords, should be backed up before upgrading or downgrading.

Table 5-53 summarizes the system behavior with regard to passwords and certificates when upgrading to or downgrading from this version.

Version Change - Password and Certificate Compatibility

Version	Behavior	
Change	Passwords	Certificates
Upgrade from old version to new version	 On user login: All new-user passwords are hashed and saved using SHA-256. Existing user passwords remain saved using the SHA-1 signature, however: On first login after the upgrade the SHA-1 hashed password is automatically replaced with SHA-256 hashed password. Note: After an upgrade to version 8.1.4.J there will be still passwords saved with the SHA-1 signature. In order not to rely on automatic password signature conversion and replacement, and to ensure that the system only has SHA-256 hashed passwords saved, the administrator should: Either: Ensure that all the users login to the system at least once to ensure automatic replacement of SHA-1 hashed passwords with SHA-256 hashed passwords. 	The new version accepts certificates issued with SHA-1 hashing.
Downgrade from new version to old version	Delete and recreate all users. Before the downgrade procedure begins, the administrator receives a popup warning message "Passwords will change to factory default would you like to proceed?" All users and SHA-256 hashed passwords are deleted. The administrator's User Name and Password reverts to the Factory Default: POLYCOM / POLYCOM.	The old version accepts certificates issued with SHA-1 hashing. For certificates issued with SHA-256 hashing: The administrator receives a popup warning message "TLS certificate will be deleted and the system will switch to non-secured connection, would you like to proceed?" For each certificate that is hashed with SHA-256: RMX Web Client / RMX Manager connections to the RMX are switched to non-secured mode. LDAP services are changed from 636 to port 389. SIP TLS sessions are changed to SIP UDP. The certificate is deleted.

Non-hashed Passwords

All non-hashed passwords are stored encrypted as set out in Table 5-54.

Non-hashed Passwords - Encryption

Connection	Storage type	Previous Versions	From Version 8.1
SNMPv3 Two passwords: Authentication / Privacy	Community permissions which are not the PW to connect to SNMP are not Saved Encrypted	Non encrypted	AES 256
Exchange	Non encrypted – Feature disabled in Ultra Secure Mode	Non encrypted	AES 256
RV v.35 serial ports – password for login	Reversible – AES_128 with 256 Bytes Key (2048 Bits)	AES 256	AES 256
H.323 authentication – password	Reversible – AES_128 with 256 Bytes Key (2048 Bits)	AES 256	AES 256
SIP digest – password	Reversible – AES_128 with 256 Bytes Key (2048 Bits)	AES 256	AES 256

In compliance with UC APL requirements, PKI Self-signed Certificates are supported for the both the Default Management and IP Network Services.

A mixture of **Self-signed** and **CA-signed Certificates** is supported, however a **CA-signed** certificate will always override a **Self-signed Certificate**.

Self-signed Certificate Creation

Self-signed Certificates are created during:

- Initial system start-up before any **CA-signed Certificates** have been installed.
- IP Network Services creation.
- Network Services updates that result in Host Name changes.
- Daily validity checks of Self-signed Certificates.
- Backup and Restore of the system configuration

Self-signed Certificate field values are automatically inserted when the certificate is created

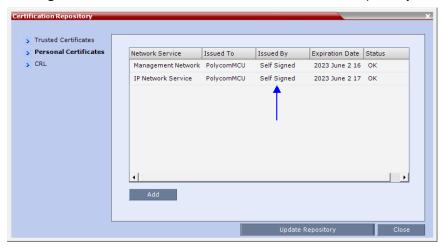
Self-signed Certificate - Creation

Field	Value
Signature Algorithm	SHA1

Self-signed Certificate - Creation

Field	Value
Issuer / Issued To	Service Host Name
	Both the Issuer and Issued To fields have the same values.
	CN = host name of the service name
	DC = Polycom
	OU = Self Signed Certificate
	O = Polycom RMX
	Note: The value of <i>CN</i> is derived from the <i>IP Network Service Name</i> , while the values of <i>DC</i> , <i>OU</i> and <i>O</i> are hard coded.
	For a full description of these fields see RFC 5280.
Valid from	Date of creation
Valid to	Date of creation + 10 years
Subject (Common Name)	Service Host Name
Public Key	2048 bits

Self-signed Certificates are indicated in the Certification Repository - Issued By field.



Media Encryption and Authentication

In compliance with UC_APL_SEC_0013, the RMX supports Privacy Protocol AES_CM_128_HMAC_SHA1_32, in addition to AES_CM_128_HMAC_SHA1_80.

System Flag

The Privacy Protocol selection is controlled by the **SRTP_SRTCP_HMAC_SHA_LENGH** System Flag. To modify its setting, manually add it to **system.cfg** and set its value as summarized in Table 5-56.

Range: 80, 32, 80_32

Default: 80

Privacy Protocols - Flag Settings

SRTP_SRTCP_HMAC_SHA_LE	Negotiation Protocol SDP	Authentication Tag Length	
NGH Flag Value		RTP	RTCP
80	AES_CM_128_HMAC_SHA1_80	80	80
32	AES_CM_128_HMAC_SHA1_32	32	80
80_32	First: AES_CM_128_HMAC_SHA1_32 Second: AES_CM_128_HMAC_SHA1_80	32 or 80 (Depending on negotiation result)	80

Collaboration Server Hardware Monitoring

The status and properties of the Collaboration Server hardware components can be viewed and monitored in the *Hardware Monitor* list pane.

Viewing the Status of the Hardware Components

The *Hardware Monitor's* status column displays the present status of the hardware components. In addition to the status, temperature and voltage indications are provided for each component.

The MCU's Shelf Management Server is what users are connecting to when accessing the *Hardware Monitor* pane. This pane can be accessed in either two ways: through the *Collaboration Server Web Client* or the Shelf Management Server. Connection via the Shelf Management Server enables users to access the *Hardware Monitor* even when the connection through the *Collaboration Server Web Client* is unavailable. The ability to connect directly via the Shelf Management Server enables users to: enter the *Hardware Monitor* and view the problematic hardware components, reset and restart the MCU and run diagnostics. Running diagnostics and restarting the MCU can only be done via direct connection to the Shelf Management Server. For more information, see Diagnostic Mode (RealPresence Collaboration Server (RMX) 1500/2000/4000)



When accessing the Shelf Management server, the content displayed will be available in English only.

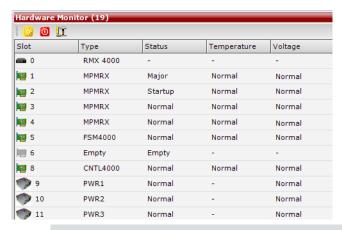


Shelf Management is not supported on the RMX 1800.

To view the status of the Hardware Components on the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000:

» In the Collaboration Server Management pane, click the Hardware Monitor button. The Hardware Monitor pane is displayed.

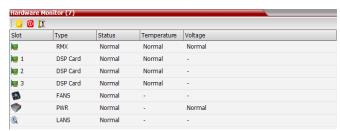
RealPresence Collaboration Server (RMX) 1500/2000/4000 Hardware Monitor Pane





In the Hardware Monitor, Slots 1 & 2 may sometimes appear as duplicates in the Slot list.

RealPresence Collaboration Server 1800Hardware Pane



The *Hardware Monitor* pane displays the following Collaboration Server hardware component's status columns:

HW Monitor Pane Status Columns

Field	Description
Slot	Displays an icon according to the HW component type and the slot number. The icon displays the hardware status as follows: • An exclamation point (!) indicates errors in the HW component. • Card icon with the reset button () indicates that the HW component is currently resetting. • Card icon with diagnostic tools () indicates that the HW component is in diagnostic mode.

Field	Description
Туре	The type of hardware component card.
Status	The current status of the HW component; Normal, Major, Critical, Resetting, Diagnostics, or Empty.
Temperature	Monitors the temperature of the hardware components; Normal, Major and Critical. Note: Critical condition invokes a system shut down.
Voltage	The voltage threshold of the hardware component; either Normal or Major.

HW Monitor Pane Toolbar

The following buttons appear in the tool bar of the Hardware Monitor:

HW Monitor Pane Tool Bar Buttons

Button	Name	Description
	System Reset	Resets and restarts the system. Resetting saves settings and information that you changed in the system, i.e. IP Services, etc
0	System Shut Down	Shuts down the system into a standby mode. When the user in the <i>Collaboration Server Manager/Client</i> presses the <i>System Shut Down</i> (red) button in the Hardware Monitor tool bar, the system should enter a standby mode and the LED turns ON. Only the media and control unit cards are in a standby mode. Shelf Manager remains active. Turn the system OFF/ON to exit the standby mode.
	System Start Up	Starts up the system. Note: This button is only displayed when connecting directly to the Shelf Management server.
	Shelf Manager	In the HW Monitor this opens the Shelf Management login window. In the Shelf Management HW Monitor this sets the MFA, CPU and Switch (Cards: MPMx/MPMRx, CNTL and RTM IP) into diagnostic mode. For more information, see Diagnostic Mode (RealPresence Collaboration Server (RMX) 1500/2000/4000).
	Logger Mode	Diagnostics Tests selection and Tests monitoring. Note: This button is only displayed when connecting directly to the Shelf Management server and logged in as a special support user.

Viewing the Properties of RealPresence Collaboration Server (RMX) 1500 Hardware Components

The properties displayed for the hardware components will vary according to the type of component viewed. These component properties can be grouped as follows:

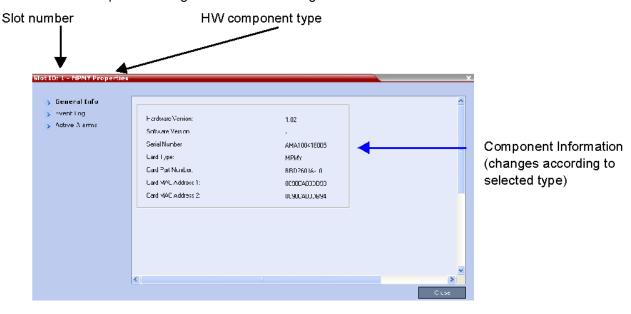
- MCU Properties (RealPresence Collaboration Server (RMX) 1500)
- Card Properties (MPMx/MPMRx, CNTL, RTM IP, RTM ISDN)

Supporting Hardware Components Properties (Backplane, FANS, LAN)



No properties are provided for Power Supply (PWR). For more information, see the *RealPresence Collaboration Server (RMX) 1500 Hardware Guide*, RMX 1500 Power Supply .

The Hardware Properties dialog box has the following structure:



To view the MCU Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **Properties** for *RMX 1500, slot 0*.



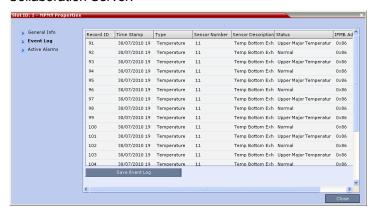
The following information is displayed:

MCU Properties - General Info

Field	Description
Chassis File ID	The ID assigned to the MCU's chassis file.

Field	Description
Chassis Serial Number	The serial number assigned to the MCU's chassis.
Part Number	The chassis part number. The Part Number contains the letter A/B/C/D that represents the chassis type.
Card Type	The name of the hardware product or component, i.e. RMX 1500, Backplane.
Chassis HW Version	Indicates the MCU's current chassis hardware version.
Turn on SSH	On - enables, Off - disables the SSH monitor. This is a secured terminal enabling access to the operating system in order to define Linux commands.

2 Click the Event Log tab to view a log of events that were recorded by the system for the Collaboration Server.

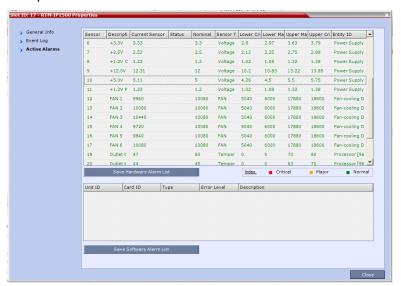


The logged events can be saved to a *.xls file by clicking the **Save Event Log** button. It is not possible to save individual or multiple selected events; the entire log file must be saved.

MCU Properties - Event Log

Column	Description
Record ID	The recorded ID number of the logged event.
Time Stamp	Lists the date and time that the event occurred.
Туре	Displays the type of event recorded in the log.
Sensor Number	The number of the LED sensor on the Collaboration Server unit.
Sensor Description	Describes which sensor the event is being logged.
Status	The sensor's active status.
Ipmb Address(hex)	Contains all the internal IPMI network addresses on the IPMB bus, i.e. 0x20 (Switch), 0x86 (MFA), etc

3 Click the *Active Alarms* tab to view alarms related to the Collaboration Server, i.e. temperatures and main power sensors.



The Active Alarms dialog box displays fields that relate to faults and errors detected on the Collaboration Server by sensors. The Active Alarms dialog box is divided into two sections: HW Alarm List and SW Alarm List.

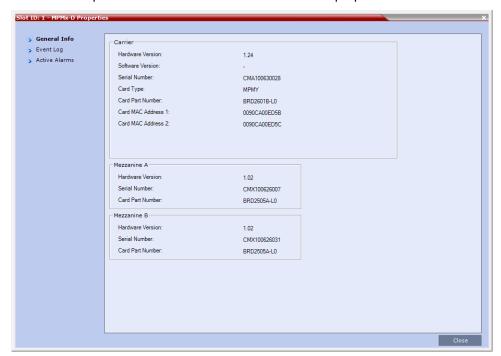
Each section's alarm list can be saved as a *.xls file by clicking the **Save HW Alarm List** and **Save SW Alarm List** buttons respectively. Each alarm list color codes the severity of the alarm; Critical (RED), Major (ORANGE) and Normal (GREEN).



If you connected to the Hardware Monitoring via the Shelf Management server, the *SW Alarm List* section will not be displayed.

To view the Card Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **properties** for the desired hardware component. Shown below is the Media card's properties.



The following information is displayed:

Card Properties - General Info

Field	Description
Hardware Version	The hardware component's version number.
Software Version	The version number of the software installed on card.
Serial Number	The hardware component's serial number.
Card Type	Displays the type of card that occupies the slot.
Card Part Number	The part number of the HW component's board.
Card Mac Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Card MAC Address 2	(If applicable) second MAC address.
Mezzanine A	
Hardware Version	The Mezzanine A hardware component's version number.

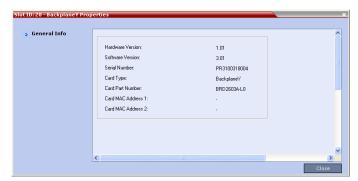
Field	Description
Serial Number	The Mezzanine A hardware component's serial number.
Card Part Number	The part number of the Mezzanine A hardware component's board.
Mezzanine B	
Hardware Version	The Mezzanine B hardware component's version number.
Serial Number	The Mezzanine B hardware component's serial number.
Card Part Number	The part number of the Mezzanine B hardware component's board.

- 2 Click the **Event Log** tab to view a log of events recorded by the system on the HW component. For more information, see To view the MCU Properties: .
- 3 Click the **Active Alarms** tab to view alarms related to the hardware component, i.e. temperatures and main power sensors.
 - For more information, see Appendix B Active Alarms .
- 4 Click Close to return to the HW Monitor pane.

To View the Supporting Hardware Components Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select properties for the desired supporting hardware component.

The component's properties dialog box will appear with the General Info tab displayed.



Backplane Properties:

The Collaboration Server unit's backplane properties provides the following information:

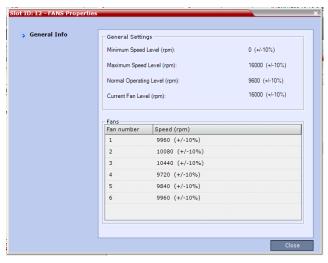
Backplane Properties - General Info

Field	Description
HW Version	The Backplane's current hardware version.
SW Version	The Backplane's current software version.
Serial Number	The Backplane's serial number.

Field	Description
Card Type	The name of the hardware component for which information is being displayed, e.g. Backplane.
Card Part Number	The Backplane's part number.
Card MAC Address 1	The Backplane's hardware address.
Card MAC Address 2	(If applicable) second Backplane MAC address.

FAN Properties:

The Collaboration Server unit's chassis contains 3 fans that regulate the unit's temperature. If the temperature increases, the fans speed will increase and vice-versa. A "Critical" condition in the fans operation will result in a system shut down.

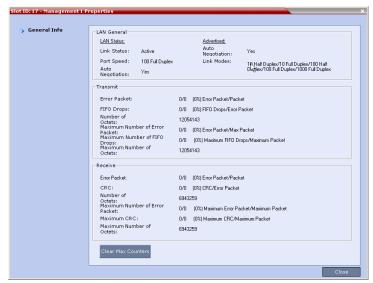


FANS Properties - General Info

Field	Description
General Settings	
Min. Speed Level (rpm)	The minimum speed level of the fans.
Max. Speed Level (rpm)	The maximum speed level of the fans.
Normal Operating Level (rpm)	The normal operating level defined for the fans.
Current Fan Level (rpm)	The current operating level of the fans.
Fans	
Fan 1 Speed (rpm)	Present speed of fan 1.
Fan 2 Speed (rpm)	Present speed of fan 2.
Fan 3 Speed (rpm)	Present speed of fan 3.

LAN 1, LAN 2, LAN 3 Properties:

The Collaboration Server unit's chassis contains 3 external LAN connectors which register the following information listed below. The information will be refreshed every 8 seconds and also contains a peek detector to log the maximal values, since the last peek values reset.



1 Click Close to return to the HW Monitor pane.

Viewing the Properties of RealPresence Collaboration Server 1800 Hardware Components

he properties displayed for the hardware components will vary according to the type of component viewed. These component properties can be grouped as follows:

- MCU Properties (RMX 1800)
- Card Properties (DSP media cards)
- Supporting Hardware Components Properties (FANS, LAN, PWR)



No properties are provided for Power Supply (PWR). For more information, see the *RealPresence Collaboration Server (RMX) 1800 Hardware Guide*, "*RealPresence Collaboration Server 1800 Specifications*" on page 2.

To view the MCU properties:

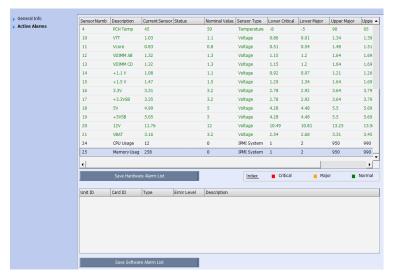


The following information is displayed:

MCU Properties - General Info

Field	Description
Hardware Version	The version of the system hardware.
Firmware Version	The version of the firmware installed on the system.
Serial Number	The serial number of the system hardware.
Card Type	Displays the type of the media card that occupies the slot.
Card Part Number	The part number of this media card.
Card MAC Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Card MAC Address 2	(If applicable) second MAC address.

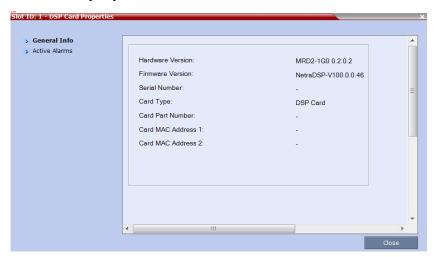
1 Click the *Active Alarms* tab to view alarms related to the Collaboration Server, i.e. temperatures and main power sensors.



The Active Alarms dialog box displays fields that relate to faults and errors detected on the Collaboration Server by sensors. The Active Alarms dialog box is divided into two sections: hardware Alarm List and SW Alarm List.

Each section's alarm list can be saved as a *.xls file by clicking the **Save HW Alarm List** and **Save SW Alarm List** buttons respectively. Each alarm list color codes the severity of the alarm: Critical (RED), Major (ORANGE) and Normal (GREEN).

To view the card properties:





The mapping between the DSP IDs and the physical slots is as the following:

- ID 1: Slot 0 (in the middle)
- ID 2: Slot 1 (bottom)
- ID 3: Slot 2 (top)

The following information is displayed:

DSP Card Properties - General Info

Field	Description
Hardware Version	The hardware component's version number.
Firmware Version	The version number of the software installed on the media card.
Serial Number	The hardware component's serial number.
Card Type	Displays the type of the media card that occupies the slot.
Card Part Number	The part number of the hardware component's board.
Card Mac Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Card MAC Address 2	(If applicable) second MAC address.

1 Click the **Active Alarms** tab to view alarms related to the hardware component, i.e. temperatures and main power sensors.

For more information, see "Active Alarms" on page 876.

2 Click **Close** to return to the *Hardware Monitor* pane.

To view the resource usage on a DSP card:

- 1 In the *Hardware Monitor* pane, double-click a desired DSP card.
- **2** The available chip list opens. You can find the following information:

DSP Card Chip Properties

Field	Description
Туре	Media type this chip is used for processing.
Configuration	
Occupied	Whether this chip is used.
Faulty	Whether this chip functions properly.
Disabled	Whether this chip is disabled.
Location	
Network Service	Which network service this chip is associated with.
Percentage Occupied	The percentage of the resource used on this chip.

3 To view the port usage of a specific chip, double-click the desired chip. You can find the following information:

DSP Chip Info

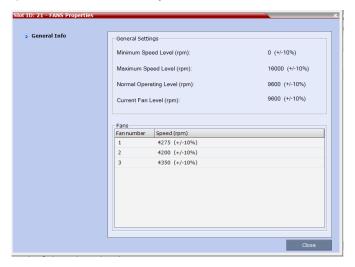
Field	Description
Port ID	The ID of the port.
Active	Whether this port is active.
Percentage Occupied	The percentage of the resource used on this chip.
Port Type	The type of this port.

To view the supporting hardware components properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select properties for the desired supporting hardware component.

The component's properties dialog box will appear with the *General Info* tab displayed. FAN Properties:

The Collaboration Server unit's chassis contains 3 fans that regulate the unit's temperature. If the temperature increases, the fans speed will increase and vice-versa. A "Critical" condition in the fans operation will result in a system shut down.

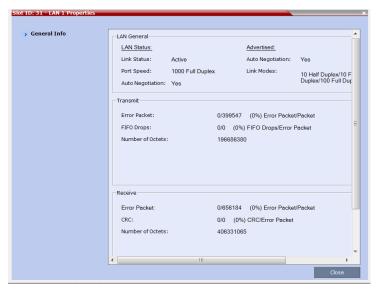


Fans Properties

Field	Description
General Settings	
Min. Speed Level (rpm)	The minimum speed level of the fans.
Max. Speed Level (rpm)	The maximum speed level of the fans.
Normal Operating Level (rpm)	The normal operating level defined for the fans.
Fans	
Fan 1 Speed (rpm)	Present speed of fan 1.
Fan 2 Speed (rpm)	Present speed of fan 2.
Fan 3 Speed (rpm)	Present speed of fan 3.

LAN 1 and LAN 2, Properties:

The Collaboration Server unit's chassis contains two external LAN connectors which register the following information listed below. The information will be refreshed every 8 seconds and also contains a peak detector to log the maximal values, since the last peak values reset.



1 Click **Close** to return to the *Hardware Monitor* pane.

Resetting the RMX 1800 DSP cards

If the DSP cards don't function properly, you can reset them during a meeting.

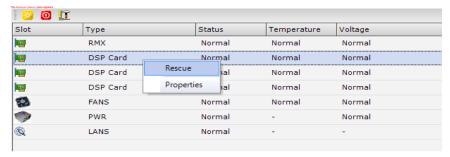
When you reset a DSP card during a meeting, the system switches the impacted meeting media to other DSP cards, if available. If no other DSP cards available, the impacted meeting media is lost and there may be few seconds' pause in the meeting video.



Only Polycom Support can reset DSP cards. For more information, contact your Polycom Support.

To reset a DSP card:

1 In the *RMX Management* pane, click the **Hardware Monitor** button.



- 2 Right-click a desired DSP card and select **Rescue**.
- 3 When asked "Are you sure you want to send the rescue command to the card?", click Yes.
 The media card resets and its Status changes to Resetting. Upon the completion of the reset, its Status changes back to Normal.

Temperature Thresholds

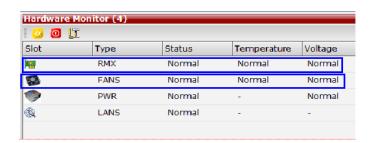
On each Collaboration Server card or there are temperature sensors that are placed near specific components on the media card. In the *Hardware Monitor* you can view the properties of each card together with their temperature statuses. By right clicking on any card and viewing the cards *Properties*, the *Active Alarms* tab displays all the card sensors, their statuses and lists each sensor's temperature specifications. When the temperature on the cards initially rises, a fault could be triggered and can viewed in the *System Alerts, Faults List.* Load issues can arise when the system nears the maximum conference mark or high port capacity occurs on an Collaboration Server resulting in *Upper Major* or *Upper Critical* faults.



With an Upper Major alarm activation it is recommended to perform the following checks: Fans/fan tray functions, Overall System Ventilation and Filter (top, bottom & sides free and no dust) and Room temperature (cool). When no apparent cause can be found, then contact your next level of support.

However, only when the *Upper Critical* threshold is passed does the Collaboration Server system as a precaution initiate a system shutdown.

RealPresence Collaboration Server (RMX) 1800 Hardware Monitor pane



Viewing the Properties of RealPresence Collaboration Server (RMX) 2000 Hardware Components

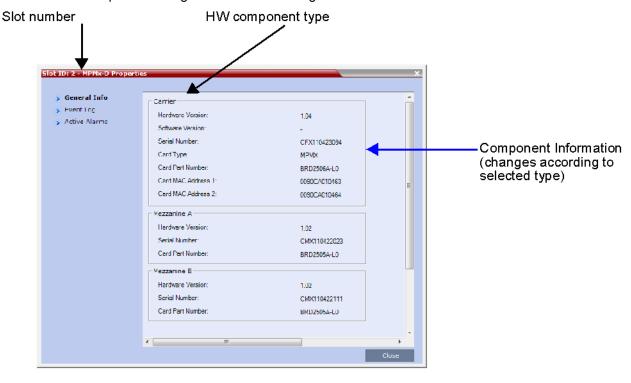
The properties displayed for the hardware components will vary according to the type of component viewed. These component properties can be grouped as follows:

- MCU Properties (RealPresence Collaboration Server (RMX) 2000)
- Card Properties (MPMx, MPMRx, CNTL, RTM IP, RTM ISDN, RTM LAN)
- Supporting Hardware Components Properties (Backplane, FANS, LAN)



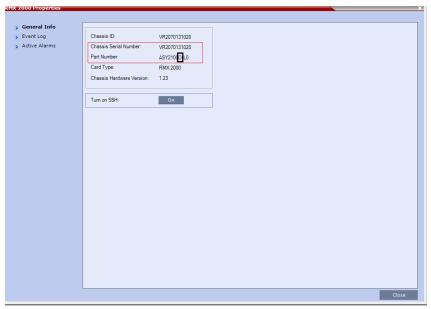
• No properties are provided for Power Supply (PWR). For more information, see the *RealPresence Collaboration Server (RMX) 2000 Hardware Guide*,.

The Hardware Properties dialog box has the following structure:



To view the MCU Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **properties** for *RMX 2000, slot 0*.

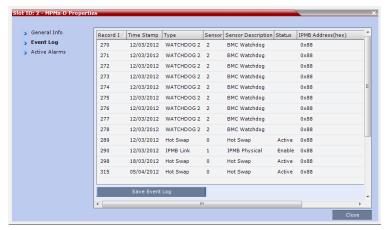


The following information is displayed:

MCU Properties - General Info

Field	Description
Chassis File ID	The ID assigned to the MCU's chassis file.
Chassis Serial Number	The serial number assigned to the MCU's chassis.
Part Number	The chassis part number. The Part Number contains the letter A/B/C/D that represents the chassis type.
Card Type	The name of the hardware product or component, i.e. RMX 2000, Backplane.
Chassis HW Version	Indicates the MCU's current chassis hardware version.
Turn on SSH	On - enables, Off - disables the SSH monitor. This is a secured terminal enabling access to the operating system in order to define Linux commands.

2 Click the *Event Log* tab to view a log of events that were recorded by the system for the Collaboration Server.



The logged events can be saved to a *.xls file by clicking the **Save Event Log** button. It is not possible to save individual or multiple selected events; the entire log file must be saved.

MCU Properties - Event Log

Column	Description
Record ID	The recorded ID number of the logged event.
Time Stamp	Lists the date and time that the event occurred.
Туре	Displays the type of event recorded in the log.
Sensor Number	The number of the LED sensor on the Collaboration Server unit.
Sensor Description	Describes which sensor the event is being logged.
Status	The sensor's active status.
Ipmb Address(hex)	Contains all the internal IPMI network addresses on the IPMB bus, i.e. 0x20 (Switch), 0x86 (MFA), etc

3 Click the Active Alarms tab to view alarms related to the Collaboration Server, i.e. temperatures and main power sensors.



The Active Alarms dialog box displays fields that relate to faults and errors detected on the Collaboration Server by sensors. The Active Alarms dialog box is divided into two sections: HW Alarm List and SW Alarm List.

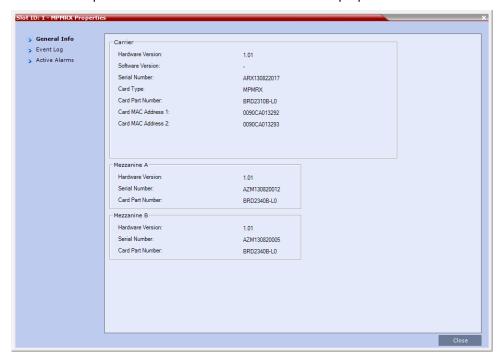
Each section's alarm list can be saved as a *.xls file by clicking the **Save HW Alarm List** and **Save SW Alarm List** buttons respectively. Each alarm list color codes the severity of the alarm; Critical (RED), Major (ORANGE) and Normal (GREEN).



If you connected to the Hardware Monitoring via the Shelf Management server, the SW Alarm List section will not be displayed.

To view the Card Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **properties** for the desired hardware component. Shown below is the Media card's properties.



The following information is displayed:

Card Properties - General Info

Field	Description
HW Version	The hardware component's version number.
SW Version	The version number of the software installed on card.
Serial Number	The hardware component's serial number.
Card Type	Displays the type of card that occupies the slot.
Card Part Number	The part number of the HW component's board.
Card MAC Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Card MAC Address 2	(If applicable) second Mac address.
Mezzanine A	Hardware Version: The hardware component's version number.
	Serial Number: The hardware component's serial number.
	Card Part Number: The part number of the HW component's subboard.

Field	Description
Mezzanine B	Hardware Version: The hardware component's version number.
	Serial Number: The hardware component's serial number.
	Card Part Number: The part number of the HW component's subboard.

2 Click the Event Log tab to view a log of events that was recorded by the system on the HW component.

For more information, see To view the MCU Properties:

3 Click the Active Alarms tab to view alarms related to the hardware component, i.e. temperatures and main power sensors.

For more information, see Appendix B - Active Alarms.

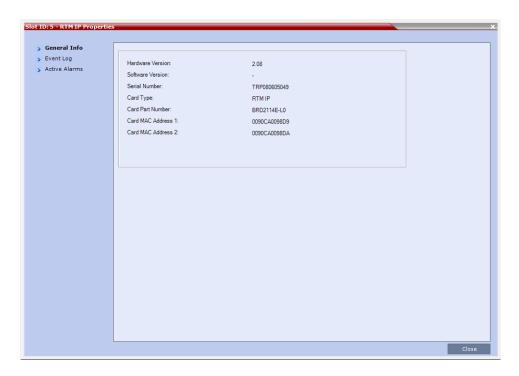
4 Click **Close** to return to the *HW Monitor* pane.

To View the Supporting Hardware Components Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select properties for the desired supporting hardware component.

The component's properties dialog box will appear with the General Info tab displayed.

RMX 2000 RTM IP Properties:



The Collaboration Server unit's RTM IP properties provides the following information:

RTM IP Properties - General Info

Field	Description
HW Version	The RTM IP's current hardware version.
SW Version	The RTM IP's current software version.
Serial Number	The RTM IP's serial number.
Card Type	The name of the hardware component for which information is being displayed, e.g. RTM IP.
Card Part Number	The RTM IP's part number.
Card Mac Address 1	The RTM IP's hardware address.
Card Mac Address 2	(If applicable) second RTM IP's Mac address.

Backplane Properties:



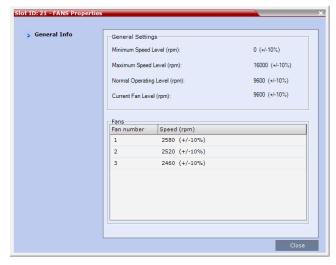
The Collaboration Server unit's backplane properties provides the following information:

Backplane Properties - General Info

Field	Description
HW Version	The Backplane's current hardware version.
SW Version	The Backplane's current software version.
Serial Number	The Backplane's serial number.
Card Type	The name of the hardware component for which information is being displayed, e.g. Backplane.
Card Part Number	The Backplane's part number.
Card Mac Address 1	The Backplane's hardware address.
Card Mac Address 2	(If applicable) second Backplane Mac address.

FAN Properties:

The Collaboration Server unit's chassis contains 3 fans that regulate the unit's temperature. If the temperature increases, the fans speed will increase and vice-versa. A "Critical" condition in the fans operation will result in a system shut down.

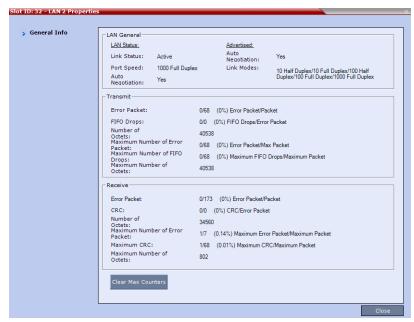


FANS Properties - General Info

Field	Description
General Settings	
Min. Speed Level (rpm)	The minimum speed level of the fans.
Max. Speed Level (rpm)	The maximum speed level of the fans.
Normal Operating Level (rpm)	The normal operating level defined for the fans.
Current Fan Level (rpm)	The current operating level of the fans.
Fans	
Fan number (1-3)	Fan numbering.
Speed (rpm)	Present speed of a fan (1-3).

LAN 0, LAN 1, LAN 2 Properties:

The Collaboration Server unit's chassis contains 3 external LAN connectors which register the following information listed below. The information will be refreshed every 8 seconds and also contains a peek detector to log the maximal values, since the last peek values reset.



1 Click **Close** to return to the *HW Monitor* pane.

Viewing the Properties of RealPresence Collaboration Server (RMX) 4000 Hardware Components

The properties displayed for the hardware components will vary according to the type of component viewed. These component properties can be grouped as follows:

- MCU Properties (RealPresence Collaboration Server (RMX) 4000)
- Card Properties (MPMx/MPMRx, CNTL 4000, RTM-IP 4000, RTM ISDN, RTM LAN)
- Supporting Hardware Components Properties (Backplane, FANS, LAN)



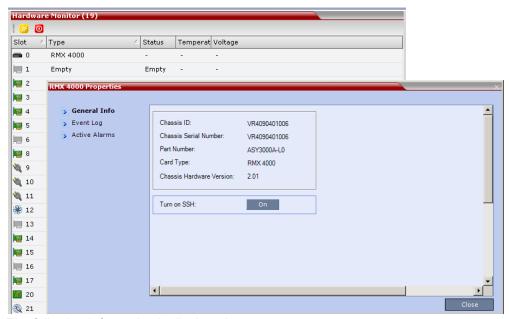
• No properties are provided for Power Supply (PWR). For more information, see the *RealPresence Collaboration Server (RMX) 4000 Hardware Guide*.

Slot number HW component type General Info > Event Log Active Alarms Software Version: Serial Number: Component ΔMΔ100418005 Card Type: MPMY Information Card Part Number: BRD2601A-L0 (changes Card MAC Address 1: 0090CA00DB93 Card MAC Address 2: according to 0090CA00DB94 selected type)

The Hardware Properties dialog box has the following structure:

To view the MCU Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **Properties** for *RMX 4000, slot 0*.



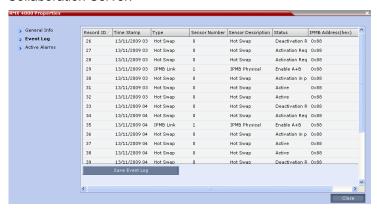
The following information is displayed:

MCU Properties - General Info

Field	Description
Chassis File ID	The ID assigned to the MCU's chassis file.
Chassis Serial Number	The serial number assigned to the MCU's chassis.

Field	Description
Part Number	The chassis part number. The Part Number contains the letter A/B/C/D that represents the chassis type.
Card Type	The name of the hardware product or component, i.e. RMX 4000, Backplane.
Chassis HW Version	Indicates the MCU's current chassis hardware version.
Turn on SSH	On - enables, Off - disables the SSH monitor. This is a secured terminal enabling access to the operating system in order to define Linux commands.

2 Click the Event Log tab to view a log of events that were recorded by the system for the Collaboration Server.

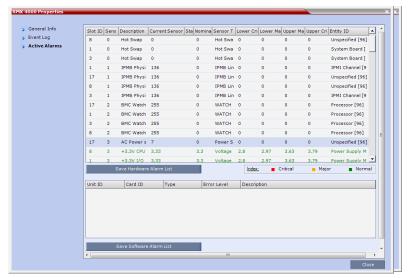


The logged events can be saved to a *.xls file by clicking the **Save Event Log** button. It is not possible to save individual or multiple selected events; the entire log file must be saved.

MCU Properties - Event Log

Column	Description
Record ID	The recorded ID number of the logged event.
Time Stamp	Lists the date and time that the event occurred.
Туре	Displays the type of event recorded in the log.
Sensor Number	The number of the LED sensor on the Collaboration Server unit.
Sensor Description	Describes which sensor the event is being logged.
Status	The sensor's active status.
Ipmb Address(hex)	Contains all the internal IPMI network addresses on the IPMB bus, i.e. 0x20 (Switch), 0x86 (MFA), etc

3 Click the *Active Alarms* tab to view alarms related to the Collaboration Server, i.e. temperatures and main power sensors.



The Active Alarms dialog box displays fields that relate to faults and errors detected on the Collaboration Server by sensors. The Active Alarms dialog box is divided into two sections: HW Alarm List and SW Alarm List.

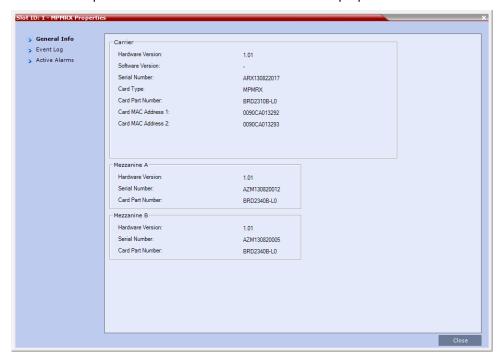
Each section's alarm list can be saved as a *.xls file by clicking the **Save HW Alarm List** and **Save SW Alarm List** buttons respectively. Each alarm list color codes the severity of the alarm; Critical (RED), Major (ORANGE) and Normal (GREEN).



If you connected to the Hardware Monitoring via the Shelf Management server, the *SW Alarm List* section will not be displayed.

To view the Card Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select **Properties** for the desired hardware component. Shown below is the Media card's properties.



The following information is displayed:

Card Properties - General Info

Field	Description
HW Version	The hardware component's version number.
SW Version	The version number of the software installed on card.
Serial Number	The hardware component's serial number.
Card Type	Displays the type of card that occupies the slot.
Board Part Number	The part number of the HW component's board.
Board Mac Address 1	Specific hardware address of the component. This address is burnt onto the component and is automatically identified by the system.
Board Mac Address 2	(If applicable) second Mac address.
Mezzanine A	Hardware Version: The hardware component's version number.
	Serial Number:The hardware component's serial number.
	Card Part Number: The part number of the HW component's subboard.

Field	Description
Mezzanine B	Hardware Version: The hardware component's version number.
	Serial Number:The hardware component's serial number.
	Card Part Number: The part number of the HW component's subboard.
Mezzanine C	Hardware Version: The hardware component's version number.
	Serial Number:The hardware component's serial number.
	Card Part Number: The part number of the HW component's subboard.
Mezzanine D	Hardware Version: The hardware component's version number.
	Serial Number:The hardware component's serial number.
	Card Part Number: The part number of the HW component's subboard.

2 Click the Event Log tab to view a log of events that was recorded by the system on the HW component.

For more information, see To view the MCU Properties: .

3 Click the **Active Alarms** tab to view alarms related to the hardware component, i.e. temperatures and main power sensors.

For more information, see Appendix B - Active Alarms.

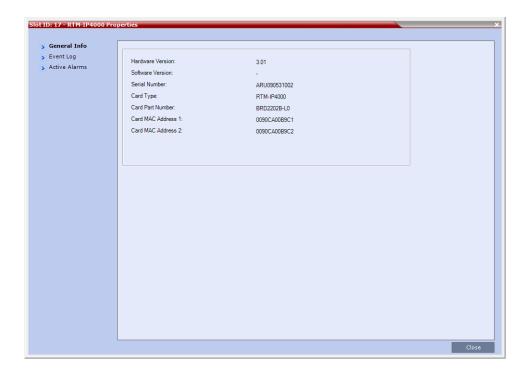
4 Click **Close** to return to the *HW Monitor* pane.

To View the Supporting Hardware Components Properties:

1 In the *Hardware Monitor* pane, either double-click or right-click and select properties for the desired supporting hardware component.

The component's properties dialog box will appear with the General Info tab displayed.

RTM IP 4000 Properties

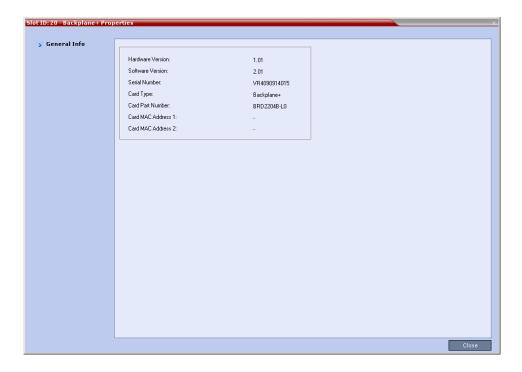


The Collaboration Server unit's RTM IP 4000 properties provides the following information:

RTP IP 4000 Properties - General Info

Field	Description
HW Version	The RTM IP's current hardware version.
SW Version	The RTM IP's current software version.
Serial Number	The RTM IP's serial number.
Card Type	The name of the hardware component for which information is being displayed, e.g. RTM IP.
Card Part Number	The RTM IP's part number.
Card Mac Address 1	The RTM IP's hardware address.
Card Mac Address 2	(If applicable) second RTM IP's Mac address.

Backplane Properties



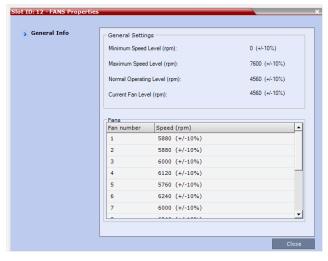
The Collaboration Server unit's backplane properties provides the following information:

Backplane Properties- General Info

Field	Description
HW Version	The Backplane's current hardware version.
SW Version	The Backplane's current software version.
Serial Number	The Backplane's serial number.
Card Type	The name of the hardware component for which information is being displayed, e.g. Backplane.
Board Part Number	The Backplane's part number.
Board Mac Address 1	The Backplane's hardware address.
Board Mac Address 2	(If applicable) second Backplane Mac address.

FAN Properties:

The Collaboration Server unit's chassis contains 3 fans that regulate the unit's temperature. If the temperature increases, the fans speed will increase and vice-versa. A "Critical" condition in the fans operation will result in a system shut down.

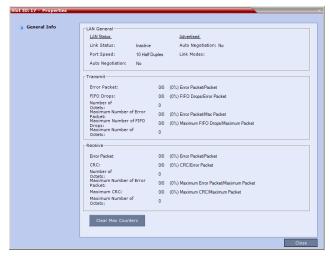


FANS Properties - General Info

Field	Description
General Settings	
Min. Speed Level (rpm)	The minimum speed level of the fans.
Max. Speed Level (rpm)	The maximum speed level of the fans.
Normal Operating Level (rpm)	The normal operating level defined for the fans.
Current Fan Level (rpm)	The current operating level of the fans.
Fans	
Fan number (1-8)	Fan numbering.
Speed (rpm)	Present speed of a fan (1-8).

LAN 0, LAN 1, LAN 2 Properties:

The Collaboration Server unit's chassis contains 3 external LAN connectors which register the following information listed below. The information will be refreshed every 8 seconds and also contains a peek detector to log the maximal values, since the last peek values reset.



» Click Close to return to the HW Monitor pane.

Diagnostic Mode (RealPresence Collaboration Server (RMX) 1500/2000/4000)

Diagnostic Mode is a debugging tool for performing hardware diagnostics that detect malfunctions in the hardware component's performance. Diagnostics are performed only for the MFA, CPU and Switch (Cards: MPMx/MPMrx, CPU, RTM IP and RTM ISDN). Two types of Diagnostic Modes are available:

- Basic Mode
- Advanced Mode

A user using an Administrator Login, will be able to view and access the *Basic Mode*. However, a Administrator "user" with Administrator permissions must be defined on the Collaboration Server system. For more information see Adding a New User . A SUPPORT user can access both the *Basic Mode* and *Advanced Mode* Diagnostics.

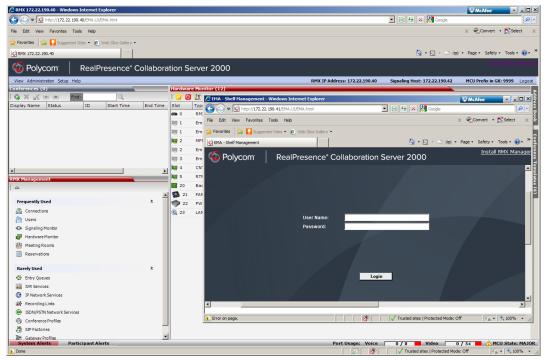
When Diagnostic Mode is initialized, the MCU is reset and upon restarting, the MCU will enter Diagnostic Mode. Entering this mode causes the MCU to terminate all active conferences and prohibits conferences from being established.

Diagnostic Mode is only enabled when connecting directly to the Shelf Management server.

Connecting to the Shelf Management Server:



- To run Diagnostics you are required to Login with Administrator permissions. A user with Administrator permissions must be defined on the Collaboration Server.
- When accessing the Shelf Management server, the content displayed will be available in English only.
- 1 Access the Collaboration Server browser and click Hardware Monitor. The Hardware Monitor pane opens.
- 2 On the Hardware Monitor toolbar click the Shelf Manager icon. Type in the URL address of the Shelf Management (IP address).
 For example; 172.22.189.51. You must also Login as an Administrator user to run diagnostics.



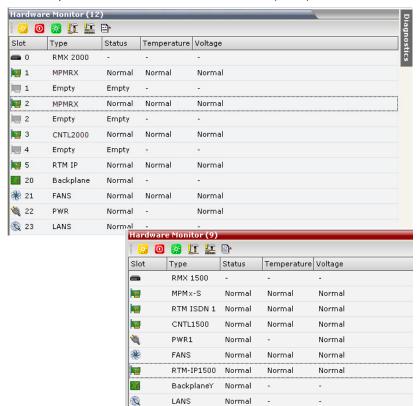
3 Login to the Shelf Manager. On the Hardware Monitor toolbar select either the Basic Mode or Advanced Mode diagnostics. Depending on your selection proceed with one of the following sections:

Performing Basic Mode Diagnostics

To run Basic Mode Diagnostics on a Hardware Component:



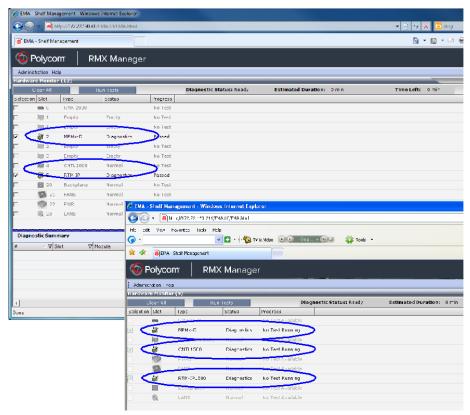
- Most of the user interfaces illustrated in this section show the RealPresence Collaboration Server (RMX) 2000 with MPMx cards. The Basic Mode for other Collaboration Servers with MPMrx cards are identical.
- On the RealPresence Collaboration Server (RMX) 1500 fewer "slots" are used and the module naming conventions used on elements are different.
- 1 In the list pane tool bar, click the **Basic Mode** () button.



2 In the Reset Confirmation dialog box, click Yes.



3 The Collaboration Server resets. Re-enter the *Shelf Manager IP address* in the browser and Login under **POLYCOM** or with an "Administrator" Login.

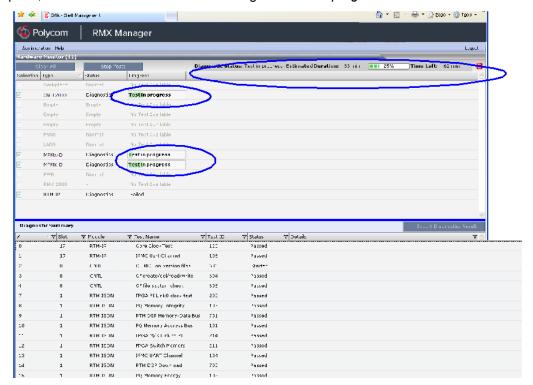


After login the following screen appears.

The MPMx/MPMrx cards indicate "Resetting" and later switch to "Diagnostics". The status of RTM-IP/RTM IP 1500/RTM-IP 4000 and CNTL/CNTL 1500/CNTL 4000 components change to "Diagnostics".

4 You can select any one of the Hardware components indicating "Diagnostics/Normal" in the status column and right-click **Properties** from the menu. The card's *General Info/Event Log/Active Alarms* properties are displayed.

5 Run Diagnostic Tests & Tests Monitoring by clicking the **Run Tests** button. In the *Hardware Monitor* pane, the toolbar and card statuses change to *Tests in progress*.



Run Tests - Parameters

Parameter	Description
Diagnostic Status	Basic Diagnostic Status: Ready - ready to run diagnostics Test in Progress - running diagnostics Passed/Failed - Passed/Failed the diagnostics tests
Estimated Duration	Estimated time needed to run Basic Diagnostic tests.
Time Left	Estimated time to complete Basic Diagnostic tests.

When the Collaboration Server enters "Diagnostics Mode", the status MPMx/MPMrx, CNTL/CNTL 1500/CNTL 4000 and RTM IP/RTM IP 1500/RTM IP 4000 changes to "Diagnostics"

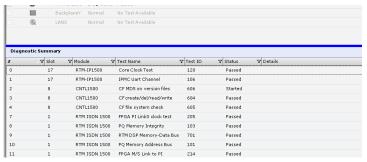
6 The *Diagnostics Summary* pane is displayed at the bottom of the *Hardware Monitoring* pane.

EMA - Shelf Management - Windows Internet Exp (3 ○) ▼ (8) http://172.22.163.248/EMA.UI/EMA.htm Ele Edit Yew Favorites Iools Help V D TV & Video Old VID TV & Video 😭 🍪 EMA - Shelf Management ↑ Tools • Polycom RMX Manager Clear All Stop Tests ction Type Z Status Progress Diagnostic Status: Test in progress Estimated Duration: 83 min | 125% | Time Left: 62 min Test in progress RTM IP Failed Diagnostic Summary △ ▼ Slot ▼ Test Name ▼ Test ID ▼ Status ▼ Details ▼ Module CNTL CF MD5 on version files 606 Started CF create/del/read/write CNTL CF file system check 605 Passed FPGA PI Link0 clock test RTM ISDN PQ Memory Integrity 103 Passed RTM DSP Memory-Data Bus 701 RTM ISDN PQ Memory Address Bus 101 Passed FPGA M/S Link to PI RTM ISDN FPGA Switch Memory 211 Passed

RealPresence Collaboration Server (RMX) 2000/4000 Diagnostics Tests & Monitoring Tests

RealPresence Collaboration Server (RMX) 1500 Diagnostics Tests & Monitoring Tests

Passed



700

7 Select the Run all Tests box and then click Run Selected Tests.

Tests Selection - Additional Test Parameters

RTM ISDN

RTM DSP Download

Parameter	Description
Loop Test	Enter the amount of times the test is to repeat itself in succession.
Stop On Failure	Stops tests upon a failure.
Run All Test	Runs all tests listed in the TestActive column for the hardware component.

- 8 The selected tests are initialized. In the Tests Monitoring pane there is an indication of the Status of the Tests.
- **9** This process may take some time. Click *Stop Running Test* to end all the diagnostic tests. The MCU completes the current test running and then stops all remaining tests.
- **10** When the Test are completed, you have the option to download a report in Excel format for analysis by your next level of support by clicking the **Export Diagnostics Result** button.
- 11 The Diagnostics Mode can be exited by pressing the red System Reset icon.
- 12 The Collaboration Server then resets.

Performing Advanced Mode Diagnostics

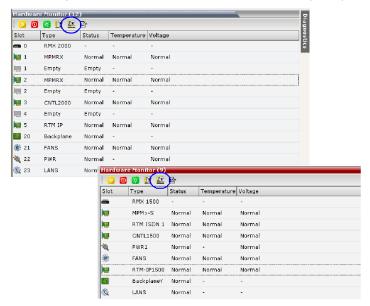


To run Diagnostics you are required to Login with administrator permissions.

To run Advanced Mode Diagnostics on a Hardware Component:



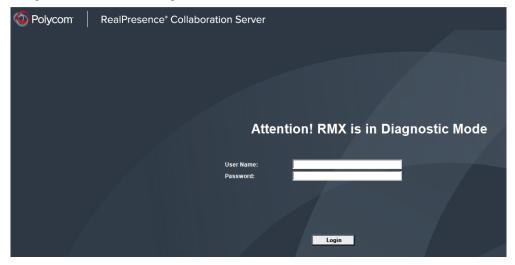
- Most of the user interfaces illustrated in this section show the RealPresence Collaboration Server (RMX) 2000 with MPMRx cards. The Advanced Mode for other Collaboration Servers with MPMx card(s) are identical.
- On the RealPresence Collaboration Server (RMX) 1500 fewer "slots" are used and the module naming conventions used on elements differ.
- Before running Advanced Mode Diagnostic testing on the CNTL module, you must insert two
 formatted FAT32 USB keys in the two slots of the CNTL panel USB ports of the RealPresence
 Collaboration Server (RMX) 2000/4000. On the RealPresence Collaboration Server (RMX) 1500
 insert the USB key in the front panel mouse or keyboard slot.
- 1 In the list pane tool bar, click the **Advanced Mode** () button.



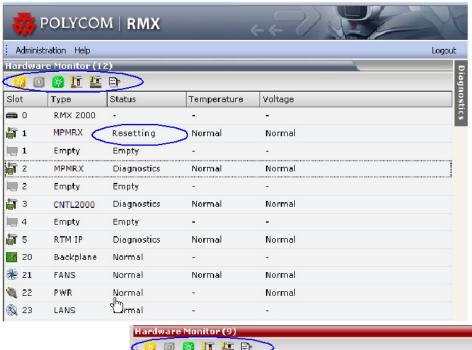
2 In the Reset Confirmation dialog box, click Yes.

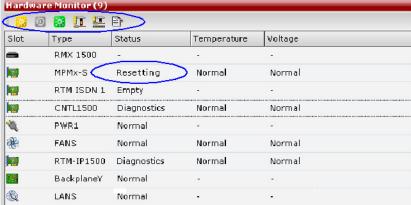


3 The Collaboration Server resets. Re-enter the *ShelfManager IP address* in the browser and Login using an "Administrator" Login.



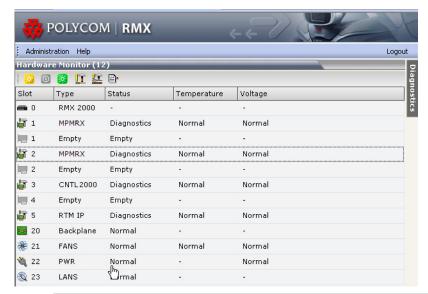
4 The MPMx/MPMRx cards indicate "Resetting" and later switch to "Diagnostics". The status of RTM-IP/RTM IP 1500/RTM-IP 4000 and CNTL/CNTL 1500/CNTL 4000 components change to "Diagnostics".





5 You can select any one of the Hardware components indicating "Diagnostics/Normal" in the status column and right-click **Properties** from the menu. The card's *General Info/Event Log/Active Alarms* properties are displayed.

You can view Diagnostic Tests & Tests Monitoring by clicking the **Diagnostics** Tab.





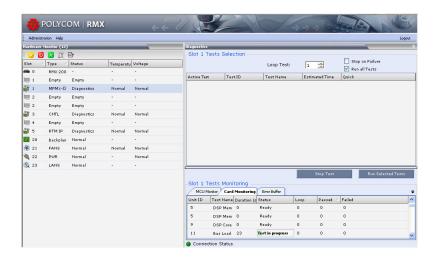
When you click the **Advanced Mode** the Collaboration Server enters a "Diagnostics Mode". The *Advanced Mode* can be exited by pressing the yellow *System Reset* icon. The Collaboration Server then resets.

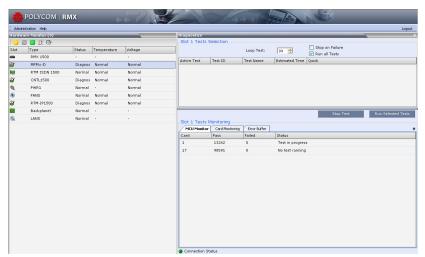
The Diagnostics Tests & Monitoring Tests panes are displayed on the right side of the window pane.



On MPMx/MPMRX and all RTM IP card types, double click each card to view details of the *Test Selection* pane as shown in step 6.

RealPresence Collaboration Server (RMX) 2000/4000 Diagnostics Tests & Monitoring Tests

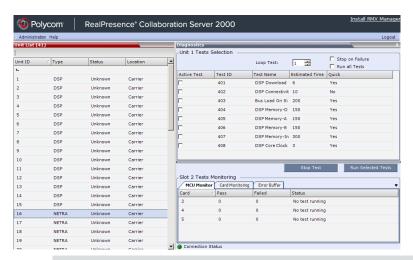




RealPresence Collaboration Server (RMX) 1500 Diagnostics Tests & Monitoring Tests

6 When the Collaboration Server enters "Diagnostics Mode", the status MPM+/MPMx, CNTL/CNTL 1500/CNTL 4000 and RTM IP/RTM IP 1500/RTM IP 4000 changes to "Diagnostics". You can run "Diagnostics" tests on an MPMx/MPMrx card by double clicking any one of the hardware components indicating "Diagnostics" in the status column.

RealPresence Collaboration Server (RMX) 2000/4000 MPMx D - DSP Sub Test selection





Run a "Diagnostics" test on a CTNL card by **clicking** the CTNL2000 hardware component that indicates "Diagnostics" in the status column.

7 Select the Run all Tests box and then click Run Selected Tests.



Optional. In the *Diagnostics - Active Test* box you can select specific tests to run and then click **Run Selected Tests**.

Tests Selection - Additional Test Parameters

Parameter	Description
Loop Test	Enter the amount of times the test is to repeat itself in succession.
Stop On Failure	Stops tests upon a failure.
Run All Test	Runs all tests listed in the TestActive column for the hardware component.

8 The selected tests are initialized. In the *Tests Monitoring* pane there is an indication of the *Connection Status* of the Tests.



Connection Status

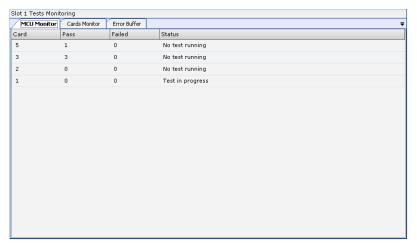
- **9** This process may take some time. Click *Stop Running Test* to end all the diagnostic tests. The MCU completes the current test running and then stops all remaining tests.
- **10** The Diagnostics Mode can be exited by pressing the yellow *System Reset* icon. The Collaboration Server then resets.

Diagnostics Monitoring

A hardware component's test status can be viewed in the Diagnostics Test Monitoring section before, during and after tests have been initiated. Test results will only be displayed after tests are completed. The Diagnostic Tests Monitoring section is comprised of three tabs: *MCU Monitor, Cards Monitor* and *Error Buffer*, which are further described below.

MCU Monitor

The MCU Monitor tab lists the status of all the cards that can be tested in Diagnostic Mode. Described below are the columns:

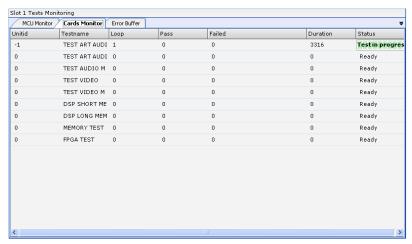


Tests Monitoring - MCU Monitor Parameters

Column	Description
Card	The card's slot number, i.e. 5 - slot where the RTM IP card resides.
Pass	Indicates the number of tests that the card passed successfully.
Fail	Indicates the number of tests that the card failed.
Status	The card's current test status: No test running or Test in progress.

Cards Monitor

The Cards Monitor tab displays the status of the selected tests being run on the currently viewed card, i.e. slot 5, described below.

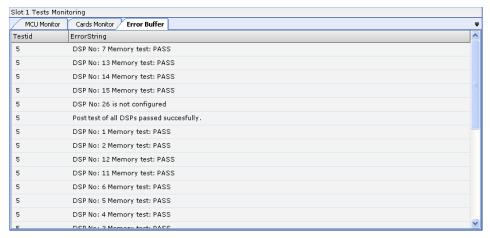


Tests Monitoring - Card Monitor Parameters

Column	Description
Unitid	The test ID number
Testname	The name of the test
Loop	Indicates the number of times the test will repeat itself in succession.
Pass	Indicates the number of times the test passed successfully.
Failed	Indicates the number of times the test failed.
Duration	The duration of the test (in seconds).
Status	The card's current test status: Test in Progress or Ready.

Error Buffer

The Error Buffer tab displays the errors encountered during testing of the cards.



Tests Monitoring - Card Monitor Parameters

Column	Description
Testid	The test ID number.
ErrorString	Indicates the error encountered during testing.

Temperature Thresholds

On each Collaboration Server card or there are temperature sensors that are placed near specific components on the card. In the *Hardware Monitor* you can view the properties of each card together with their temperature statuses. By right clicking on any card and viewing the cards *Properties*, the *Active Alarms* tab displays all the card sensors, their statuses and lists each sensor's temperature specifications. When

the temperature on the cards initially rises, a fault could be triggered and can viewed in the *System Alerts*, *Faults List*. Load issues can arise when the system nears the maximum conference mark or high port capacity occurs on an Collaboration Server resulting in *Upper Major* or *Upper Critical* faults.



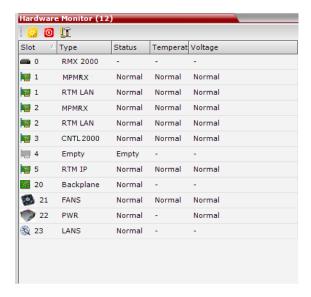
With an Upper Major alarm activation it is recommended to perform the following checks: Fans/fan tray functions, Overall System Ventilation and Filter (top, bottom & sides free and no dust) and Room temperature (cool). When no apparent cause can be found, then contact your next level of support.

However, only when the *Upper Critical* threshold is passed does the Collaboration Server system as a precaution initiate a system shutdown.



Upper Major and *Upper Critical* threshold values have sometimes also been altered, allowing for more efficient fan RPM and effective temperature management the Collaboration Server.

RealPresence Collaboration Server (RMX) 2000 Hardware Monitor pane





The Hardware Monitor view is similar on any other Collaboration Server system.

Collaboration Server RTM-IP 1500/RTM-IP/RTM IP 4000 Card Properties

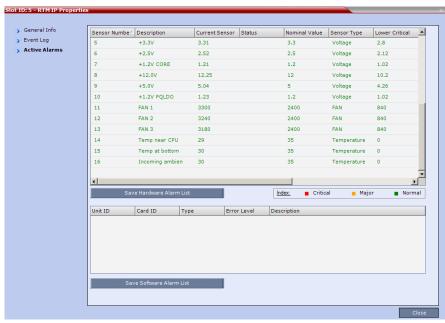
To view the Collaboration Server RTM-IP 1500/RTM-IP/RTM IP 4000 Properties:

1 In the Hardware Monitor pane, right-click the RTM IP entry and then select Properties.



Right clicking on any Collaboration Server card will display the cards *Properties*.

2 Click Active Alarms.



The RTM-IP is populated with 4 temperature sensors numbered: Sensor 14-17.



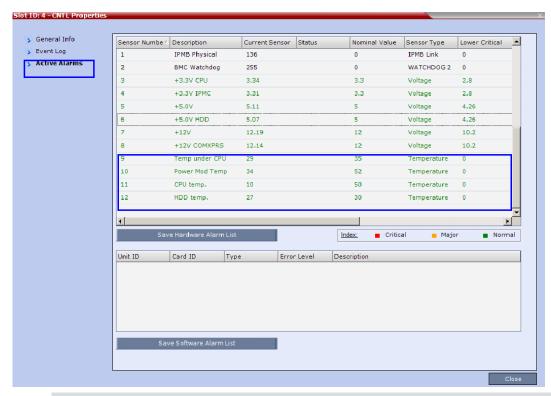
The Sensor numbering and Temperature listings may vary on Collaboration Server systems depending on card's Hardware Version and Software Version number. The Collaboration Server Manager and RealPresence Collaboration Server Client software version can also affect the UI or change the look & feel.

On the Slot ID: 5 - RTM - IP Properties, Sensor 16 is called "Incoming ambient" and on the right side of the table and you can see the threshold numbers of the sensor. For example, on Sensor 14, the event "Upper Major" is activated when the temperature reaches +60° (degrees) Centigrade. The "Upper Major" event results in an alarm being triggered. Perform an overall system check. The Upper Critical event is activated when the temperature reaches a +71° (degrees) Centigrade.

CNTL Card Properties

To view the Collaboration Server CTNL Properties:

- 1 In the Hardware Monitor pane, right-click the CTNL entry and then select Properties.
- 2 Click Active Alarms.



RealPresence Collaboration Server (RMX) 2000 CNTL Temperature Sensors



The *Sensor* numbering and *Temperature* listings may vary on Collaboration Server systems depending on card's *Hardware Version* and *Software Version* number. The *Collaboration Server Manager* and RealPresence Collaboration Server Client software version can also affect the UI or change the look & feel.

The "Upper Major" event results in an alarm being triggered. Perform an overall system check. If a temperature sensors reaches and passes "Upper Critical" then the Shelf Manager initiates a shutdown on the over-heated CNTL card.

MPMx Card Properties

To view the MPMx Properties:

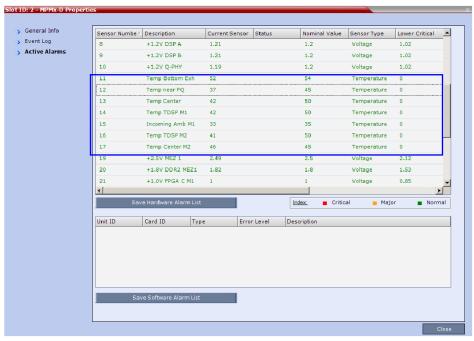
1 In the Hardware Monitor pane, right-click the MPMx entry and then select Properties.



Right clicking on any Collaboration Server MPMx card will display the cards *Properties*.

2 Click Active Alarms.

RealPresence Collaboration Server (RMX) 2000 MPMx80 Properties



The MPMx card has 7 temperature sensors numbered: 11-17, for example, when sensor 13 reaches 70° (degrees) Centigrade, it triggers an "Upper Major" event.



The Sensor numbering and Temperature listings may vary on Collaboration Server systems depending on card's Hardware Version and Software Version number. The Collaboration Server Manager and RealPresence Collaboration Server Client software version can also affect the UI or change the look & feel.

The "Upper Major" event results in an alarm being triggered. Perform an overall system check. If a temperature sensors reaches and passes "Upper Critical" then the Shelf Manager initiates a shutdown on the over-heated CNTL card.

Appendix A - Disconnection Causes

If a participant was unable to connect to a conference or was disconnected from a conference, the **Connection Status** tab in the *Participant Properties* dialog box indicates the call disconnection cause. In some cases, a possible solution may be displayed.

A video participant who is unable to connect the video channels, but is able to connect as an audio only participant, is referred to as a Secondary participant. For Secondary participants, the **Connection Status** tab in the *Participant Properties* dialog box indicates the video disconnection cause. In some cases, a possible solution may be indicated.

The table below lists the call disconnection causes that can be displayed in the Call Disconnection Cause field and provides an explanation of each message

IP Disconnection Causes

Call Disconnection Causes

Disconnection Cause	Description
Disconnected by User	The user disconnected the endpoint from the conference.
Remote device did not open the encryption signaling channel	The endpoint did not open the encryption signaling channel.
Remote devices selected encryption algorithm does not match the local selected encryption algorithm	The encryption algorithm selected by the endpoint does not match the MCU's encryption algorithm.
Resources deficiency	Insufficient resources available.
Call close. Call closed by MCU	The MCU disconnected the call.
H323 call close. No port left for audio	Insufficient audio ports.
H323 call close. No port left for video	The required video ports exceed the number of ports allocated to video in fixed ports.
H323 call close. No port left for FECC	The required data ports exceed the number of ports allocated to data in fixed ports.
H323 call close. No control port left	The required control ports exceed the number of ports allocated to control data in fixed ports.
H323 call close. No port left for videocont	The required video content ports exceed the number of ports allocated to video content in fixed ports.

Disconnection Cause	Description
H323 call closed. Small bandwidth	The gatekeeper allocated insufficient bandwidth to the connection with the endpoint.
H323 call closed. No port left	There are no free ports left in the IP card.
Caller not registered	The calling endpoint is not registered in the gatekeeper.
H323 call closed. ARQ timeout	The endpoint sent an ARQ message to the gatekeeper, but the gatekeeper did not respond before timeout.
H323 call closed. DRQ timeout	The endpoint sent a DRQ message to the gatekeeper, but the gatekeeper did not respond before timeout.
H323 call closed. Alt Gatekeeper failure	An alternate gatekeeper failure occurred.
H323 call closed. Gatekeeper failure	A gatekeeper failure occurred.
H323 call closed. Remote busy	The endpoint was busy. (Applicable only to dial-out)
H323 call closed. Normal	The call ended normally, for example, the endpoint disconnected.
H323 call closed. Remote reject	The endpoint rejected the call.
H323 call closed. Remote unreachable	The call remained idle for more than 30 seconds and was disconnected because the destination device did not answer. Possible causes can be due to network problems, the gatekeeper could not find the endpoint's address, or the endpoint was busy or unavailable (for example, the "do not disturb" status is selected).
H323 call closed. Unknown reason	The reason for the disconnection is unknown, for example, the endpoint disconnected without giving a reason.
H323 call closed. Faulty destination address	Incorrect address format.
H323 call closed. Small bandwidth	The gatekeeper allocated insufficient bandwidth to the connection with the endpoint.
H323 call closed. Gatekeeper reject ARQ	The gatekeeper rejected the endpoint's ARQ.
H323 call closed. No port left	There are no ports left in the IP card.
H323 call closed. Gatekeeper DRQ	The gatekeeper sent a DRQ.
H323 call closed. No destination IP address	For internal use.
H323 call. Call failed prior or during the capabilities negotiation stage	The endpoint did not send its capabilities to the gatekeeper.
H323 call closed. Audio channels didn't open before timeout	The endpoint did not open the audio channel.
H323 call closed. Remote sent bad capability	There was a problem in the capabilities sent by the endpoint.

Disconnection Cause	Description
H323 call closed. Local capability wasn't accepted by remote	The endpoint did not accept the capabilities sent by the gatekeeper.
H323 failure	Internal error occurred.
H323 call closed. Remote stop responding	The endpoint stopped responding.
H323 call closed. Master slave problem	A People + Content cascading failure occurred.
SIP bad name	The conference name is incompatible with SIP standards.
SIP bad status	A general IP card error occurred.
SIP busy everywhere	The participant's endpoints were contacted successfully, but the participant is busy and does not wish to take the call at this time.
SIP busy here	The participant's endpoint was contacted successfully, but the participant is currently not willing or able to take additional calls.
SIP capabilities don't match	The remote device capabilities are not compatible with the conference settings.
SIP card rejected channels	The IP card could not open the media channels.
SIP client error 400	The endpoint sent a SIP Client Error 400 (Bad Request) response. The request could not be understood due to malformed syntax.
SIP client error 402	The endpoint sent a SIP Client Error 402 (Payment Required) response.
SIP client error 405	The endpoint sent a SIP Client Error 405 (Method Not Allowed) response. The method specified in the Request-Line is understood, but not allowed for the address identified by the Request-URI.
SIP client error 406	The endpoint sent a SIP Client Error 406 (Not Acceptable) resources. The remote endpoint cannot accept the call because it does not have the necessary responses. The resource identified by the request is only capable of generating response entities that have content characteristics not acceptable according to the Accept header field sent in the request.
SIP client error 407	The endpoint sent a SIP Client Error 407 (Proxy Authentication Required) response. The client must first authenticate itself with the proxy.
SIP client error 409	The endpoint sent a SIP Client Error 409 (Conflict) response. The request could not be completed due to a conflict with the current state of the resource.
SIP client error 411	The endpoint sent a SIP Client Error 411 (Length Required) response. The server refuses to accept the request without a defined Content Length.

Disconnection Cause	Description
SIP client error 413	The endpoint sent a SIP Client Error 413 (Request Entity Too Large) response.
	The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
SIP client error 414	The endpoint sent a SIP Client Error 414 (Request-URI Too Long) response.
	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
SIP client error 420	The endpoint sent a SIP Client Error 420 (Bad Extension) response. The server did not understand the protocol extension specified in a Require header field.
SIP client error 481	The endpoint sent a SIP Client Error 481 (Call/Transaction Does Not Exist) response.
SIP client error 482	The endpoint sent a SIP Client Error 482 (Loop Detected) response.
SIP client error 483	The endpoint sent a SIP Client Error 483 (Too Many Hops) response.
SIP client error 484	The endpoint sent a SIP Client Error 484 (Address Incomplete) response.
	The server received a request with a To address or Request-URI that was incomplete.
SIP client error 485	The endpoint sent a SIP Client Error 485 (Ambiguous) response. The address provided in the request (Request-URI) was ambiguous.
SIP client error 488	The endpoint sent a SIP Client Error 488 (Not Acceptable Here) response.
SIP forbidden	The SIP server rejected the request.
	The server understood the request, but is refusing to fulfill it.
SIP global failure 603	A SIP Global Failure 603 (Decline) response was returned. The participant's endpoint was successfully contacted, but the participant explicitly does not wish to or cannot participate.
SIP global failure 604	A SIP Global Failure 604 (Does Not Exist Anywhere) response was returned.
	The server has authoritative information that the user indicated in the Request-URI does not exist anywhere.
SIP global failure 606	A SIP Global Failure 606 (Not Acceptable) response was returned.
SIP gone	The requested resource is no longer available at the Server and no forwarding address is known.
SIP moved permanently	The endpoint moved permanently. The user can no longer be found at the address in the Request-URI.
SIP moved temporarily	The remote endpoint moved temporarily.

Disconnection Cause	Description
SIP not found	The endpoint was not found. The server has definitive information that the user does not exist at the domain specified in the Request-URI.
SIP redirection 300	A SIP Redirection 300 (Multiple Choices) response was returned.
SIP redirection 305	A SIP Redirection 305 (Use Proxy) response was returned. The requested resource MUST be accessed through the proxy given by the Contact field.
SIP redirection 380	A SIP Redirection 380 (Alternative Service) response was returned. The call was not successful, but alternative services are possible.
SIP remote cancelled call	The endpoint canceled the call.
SIP remote closed call	The endpoint ended the call.
SIP remote stopped responding	The endpoint is not responding.
SIP remote unreachable	The endpoint could not be reached.
SIP request terminated	The endpoint terminated the request. The request was terminated by a BYE or CANCEL request.
SIP request timeout	The request was timed out.
SIP server error 500	The SIP server sent a SIP Server Error 500 (Server Internal Error) response. The server encountered an unexpected condition that prevented it from fulfilling the request.
SIP server error 501	The SIP server sent a SIP Server Error 501 (Not Implemented) response. The server does not support the functionality required to fulfill the request.
SIP server error 502	The SIP server sent a SIP Server Error 502 (Bad Gateway) response. The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
SIP server error 503	The SIP server sent a SIP Server Error 503 (Service Unavailable) response. The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server.
SIP server error 504	The SIP server sent a SIP Server Error 504 (Server Time-out) response. The server did not receive a timely response from an external server it accessed in attempting to process the request.

Disconnection Cause	Description
SIP server error 505	The SIP server sent a SIP Server Error 505 (Version Not Supported) response.
	The server does not support, or refuses to support, the SIP protocol version that was used in the request.
SIP temporarily not available	The participant's endpoint was contacted successfully but the participant is currently unavailable (e.g., not logged in or logged in such a manner as to preclude communication with the participant).
SIP remote device did not respond in the given time frame	The endpoint did not respond in the given time frame.
SIP trans error TCP Invite	A SIP Invite was sent via TCP, but the endpoint was not found.
SIP transport error	Unable to initiate connection with the endpoint.
SIP unauthorized	The request requires user authentication.
SIP unsupported media type	The server is refusing to service the request because the message body of the request is in a format not supported by the requested resource for the requested method.

ISDN Disconnection Causes

ISDN Disconnection Causes

Disconnection Cause		
Number	Summary	Description
1	Unallocated (unassigned number)	No route to the number exists in the ISDN network or the number was not found in the routing table. • Ensure that the number appears in the routing table. • Ensure that it is a valid number and that correct digits were dialed.
2	No route to specified transit network (national use)	The route specified (transit network) between the two networks does not exist.
3	No route to destination	No physical route to the destination number exists although the dialed number is in the routing plan. The PRI D-Channel is malfunctioning. Incorrect connection of the span or WAN.
4	Send special information tone	Return the special information tone to the calling party indicating that the called user cannot be reached.
5	Misdialed trunk prefix (national use)	A trunk prefix has erroneously been included in the called user number.
6	Channel Unacceptable	The sending entity in the call does not accept the channel most recently identified.

Disconnection Cause		
Number	Summary	Description
7	Call awarded and being delivered in an Established channel	The incoming call is being connected to a channel previously established for similar calls.
8	Pre-Emption	The call has been pre-empted.
9	Pre-Emption – Circuit reserved for reuse	Call is being cleared in response to user request.
16	Normal Call Clearing	Call cleared normally because user hung up.
17	User Busy	Dialed number is busy.
18	No User Responding	The called user has not answered the call.
19	No Answer from User (User Alerted)	Called user has received call alert, but has not responded within a prescribed period of time. Internal network timers may initiate this disconnection.
20	Subscriber Absent	User is temporarily absent from the network - as when a mobile user logs off.
21	Call Rejected	Called number is either busy or has compatibility issues. Supplementary service constraints in the network may also initiate the disconnection.
22	Number Changed	Same as Cause 1. The diagnostic field contains the new called user number. Cause 1 is used if the network does not support this cause value.
26	Non-Selected User Clearing	The incoming call has not been assigned to the user.
27	Destination Out-of-Order	Messages cannot be sent to the destination number because the span may not be active.
28	Invalid Number Format (address incomplete)	The Type of Number (TON) is incorrect or the number is incomplete. Network, Unknown and National numbers have different formats.
29	Facility Rejected	User requested supplementary service which cannot be provided by the network.
30	Response to STATUS ENQUIRY	A STATUS message has been received in response to a prior STATUS ENQUIRY.
31	Normal, Unspecified	A normal, unspecified disconnection has occurred.
34	No Circuit/Channel Available	No B-Channels are available for the call.
38	Network Out-of-Order	Network is out-of-order because due to a major malfunction.
39	Permanent Frame Mode Connection Out-of-Service	A permanent frame mode connection is out-of-service. This cause is part of a STATUS message.

Disconnection Cause		
Number	Summary	Description
40	Permanent Frame Mode Connection Operational	A permanent frame mode connection is operational. This cause is part of a STATUS message.
41	Temporary Failure	Minor network malfunction. Initiate call again.
42	Switching Equipment Congestion	High traffic has congested the switching equipment. Cause 43 is included.
43	Access Information Discarded	Access Information elements exceed maximum length and have been discarded. Included with Cause 42.
44	Requested Circuit/Channel not Available	The requested circuit or channel is not available. Alternative circuits or channels are not acceptable.
47	Resource Unavailable, Unspecified	The resource is unavailable. No other disconnection cause applies.
49	Quality of Service Not Available	Quality of Service, as defined in Recommendation X.213, cannot be provided.
50	Requested Facility Not Subscribed	A supplementary service has been requested that the user is not authorized to use.
53	Outgoing Calls Barred Within Closed User Group (CUG)	Outgoing calls are not permitted for this member of the CUG.
55	Incoming Calls Barred within CUG	Incoming calls are not permitted for this member of the CUG.
57	Bearer Capability Not Authorized	A bearer capability has been requested that the user is not authorized to use.
58	Bearer Capability Not Presently Available	A bearer capability has been requested that the user is not presently available.
62	Inconsistency in Designated Outgoing Access Information and Subscriber Class	Outgoing Access and Subscriber Class information is inconsistent
63	Service or Option Not Available, Unspecified	The service or option is unavailable. No other disconnection cause applies.
65	Bearer Capability Not Implemented	The requested bearer capability is not supported.
66	Channel Type Not Implemented	The requested channel type is not supported.
69	Requested Facility Not Implemented	The requested supplementary service is not supported.

Disconnec	Disconnection Cause		
Number	Summary	Description	
70	Only Restricted Digital Information Bearer Capability is Available (national use)	Unrestricted (64kb) bearer service has been requested but is not supported by the equipment sending this cause.	
79	Service or Option Not Implemented, Unspecified	An unsupported service or unimplemented option has been requested. No other disconnection cause applies.	
81	Invalid Call Reference Value	A message has been received which contains a call reference which is currently unassigned or not in use on the user-network interface.	
82	Identified Channel Does Not Exist	A request has been received to use a channel which is currently inactive or does not exist.	
83	A Suspended Call Exists, but This Call Identity Does Not Exist	A RESUME message cannot be executed by the network as a result of an unknown call identity.	
84	Call Identity in Use	A SUSPEND message has been received with a call identity sequence that is already in use.	
85	No Call Suspended	A RESUME message cannot be executed by the network as a result of no call suspended.	
86	Call Having the Requested Call Identity Has Been Cleared	A RESUME message cannot be executed by the network as a result of the call having been cleared while suspended.	
87	User Not Member of CUG	A CUG member was called by a user who is not a member of the CUG or a CUG call was made to a non CUG member.	
88	Incompatible Destination	User-to-user compatibility checking procedures in a point-to-point data link have determined that an incompatibility exists between Bearer capabilities.	
90	Non-Existent CUG	CUG does not exist.	
91	Invalid Transit Network Selection (national use)	The transit network selection is of an incorrect format. No route (transit network) exists between the two networks.	
95	Invalid Message, Unspecified	Invalid message received. No other disconnection cause applies.	
96	Mandatory Information Element is Missing	A message was received with an information element missing.	
97	Message Type Non-Existent or Not Implemented	A message was received that is of a type that is not defined or of a type that is defined but not implemented.	

Disconnection Cause		
Number	Summary	Description
98	Message is Not Compatible with the Call State, or the Message Type is Non-Existent or Not Implemented	An unexpected message or unrecognized message incompatible with the call state has been received
99	An Information Element or Parameter Does Not Exist or is Not Implemented	A message was received containing elements or parameters that are not defined or of a type that is defined but not implemented.
100	Invalid Information Element Contents	A message other than SETUP, DISCONNECT, RELEASE, or RELEASE COMPLETE has been received which has one or more mandatory information elements containing invalid content.
101	The Message is Not Compatible with the Call State	A STATUS message indicating any call state except the Null state has been received while in the Null state.
102	Recovery on Timer Expired	An error handling procedure timer has expired.
103	Parameter Non-Existent or Not Implemented – Passed On (national use)	A message was received containing parameters that are not defined or of a type that is defined but not implemented.
110	Message with Unrecognized Parameter Discarded	A message was discarded because it contained a parameter that was not recognized.
111	Protocol Error, Unspecified	A protocol error has occurred. No other disconnection cause applies.
127	Interworking, Unspecified	An interworking call has ended.

Appendix B - Active Alarms

Active Alarms

Alarm Code	Alarm Description
A matching activation key is required. To cancel the upgrade process, reset the Collaboration Server	The system upgrade requires that a valid activation key be entered. If none is available, resetting the Collaboration Server will cancel the upgrade and return the Collaboration Server to the previous version.
A new activation key was loaded. Reset the system.	A new activation key was loaded: Reset the MCU.
A new version was installed. Reset the system.	A new version was installed: Reset the MCU.
Alarm generated by a Central Signaling component	A system alert was generated by a component of the Central Signaling.
Alarm generated by an internal component	A system alert was generated by an internal system component.
Allocation mode was modified	
Automatic reset is unavailable in Safe Mode	The system switches to safe mode if many resets occur during startup. To prevent additional resets, and allow the system to complete the startup process the automatic system resets are blocked.
Backup of audit files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that audit files need to be backed up.
Backup of CDR files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that CDR files need to be backed up.
Backup of log files is required	If the ENABLE_CYCLIC_FILE_SYSTEM_ALARMS is set to YES (default setting when ULTRA_SECURE_MODE System Flag is set to YES) and a Cyclic File reaches a file retention time or file storage capacity limit, the user is alerted that log files need to be backed up.
Bios version is not compatible with Ultra Secure Mode.	The current BIOS version is not compatible with Ultra Secure Mode (ULTRA_SECURE_MODE=YES).
Card configuration avent	

Card configuration event

Alarm Code	Alarm Description
Card failed to switch to Enhanced Secure Mode	Card failure occurred when the system was set to Ultra Secure Mode (ULTRA_SECURE_MODE=YES).
Card failure	Possible reasons for the card failure: Resetting Card Resetting component Unknown shelf error Unknown card error
Card not found	This occurs when: the system does not receive an indication about the card (since it does not exist) usually when the card was removed from the MCU and the system did not have a chance to recalculate it resources.
Card not responding	Possible reasons for the card not responding: No connection with MPM card. No connection with the Switch.
Cards wrong file's mode	
Central signaling component failure	 Central signaling component failure; unit type: [NonComponent\CSMngnt\CSH323\CSSIP] Central signaling component failure; unit type: (invalid: [NonComponent\CSMngnt\CSH323\CSSIP]) Central signaling component failure - Invalid failure type. Unit id: [id], Type: [NonComponent\CSMngnt\CSH323\CSSIP], Status: [Ok\Failed\Recovered] Central signaling component failure - Invalid failure type
Central Signaling indicating Faulty status	Central signaling failure detected in IP Network Service.
Central Signaling indicating Recovery status	
Central Signaling startup failure	Central Signaling component is down.
Conference Encryption Error	
Configuration of external database did not complete.	Check the configuration of the external DB.
Could not complete MPM Card startup procedure	Possible explanations: Unit loading confirmation was not received. No Media IP for this card. Media IP Configuration confirmation was not received. Unspecified problem. Check the card slot and reset the card.

Alarm Code	Alarm Description
Could not complete RTM ISDN Card startup procedure	The RTM ISDN card cannot complete its startup procedure (usually after system reset).
	Check the card slot and reset the card.
CPU IPMC software was not updated.	Turn off the MCU and then turn it on.
CPU slot ID not identified	The CPU slot ID required for Ethernet Settings was not provided by the Shelf Management.
D channel cannot be established	
DEBUG mode enabled	Possible explanations: • System is running in DEBUG mode.
	System DEBUG mode initiated.
	In this mode, additional prints are added and Startup and Recovery Conditions are different then Non Debug Mode.
	Change the DEBUG_MODE flag value to NO and reset the Collaboration Server.
DEBUG mode flags in use	The system is using the DEBUG CFG flags.
DMA not supported by IDE device	Possible explanations:
	 DMA (direct memory access) not supported by IDE device: Incompatible flash card / hard disk being used.
	 Flash card / hard drive are not properly connected to the board / one of the IDE channels is disconnected.
	DMA was manually disabled for testing.
DNS configuration error	Check the DNS configuration.
DNS not configured in IP Network Service	Configure the DNS in the IP Network Services.
Encryption Server Error. Failed to generate the encryption key	FIPS 140 test failed while generating the new encryption key.
Error in external database certificate	
Error reading MCU time	Failed to read MCU time configuration file ([status]).
	Manually configure the MCU Time in the Collaboration Server Web Client or RMX Manager Manager application.
eUserMsgCode_Cs_EdgeServerDnsF ailed	
eUserMsgCode_Cs_SipTLS_Certificat eHasExpired	
eUserMsgCode_Cs_SipTLS_Certificat eSubjNameIsNotValid_Or_DnsFailed	
eUserMsgCode_Cs_SipTLS_Certificat eWillExpireInLessThanAWeek	

Alarm Code	Alarm Description
eUserMsgCode_Cs_SipTLS_FailedTo LoadOrVerifyCertificateFiles	
eUserMsgCode_Cs_SipTLS_Registrat ionHandshakeFailure	
eUserMsgCode_Cs_SipTLS_Registrat ionServerNotResponding	
Event Mode Conferencing resources deficiency due to inappropriate license. Please install a new license	
External NTP servers failure	The MCU could not connect to any of the defined NTP server for synchronization due to the remote server error or network error or configuration error. Change the configuration of the NTP server.
Failed to access DNS server	Failed to access DNS server.
Failed to configure the Media card IP address	Possible reasons for the failure: Failure type: [OK Or Not supported. Does not exist Or IP failure. Duplicate IP Or DHCP failure. VLAN failure Or Invalid: [status_Number].
Failed to configure the Users list in Linux	The authentication process did not start. Use the Restore to factory Defaults to recover.
Failed to connect to application server	Possible reasons for the failure: • Failed to connect to application server: • Failed to establish connection to server, url = [url].
Failed to connect to recording device	The MCU could not connect to the defined recording device due to configuration error or network error.
Failed to connect to SIP registrar	Cannot establish connection with SIP registrar.
Failed to create Default Profile	Possible reasons for the failure: Failed to validate the default Profile. Failed to add the default Profile. Possible action: Restore the Collaboration Server configuration from the Backup. Use the Non-Comprehensive Restore To Factory Defaults operation.
Failed to initialize system base mode	
Failed to initialize the file system	Possible reasons for the failure: • Failed to initialize the file system. • Failed to initialize the file system and create the CDR index. Reset the MCU.

Alarm Code	Alarm Description
Failed to open Users list file	Restore the MCU configuration or re-define the user.
Failed to register with DNS server	Check the DNS configuration.
Failed to subscribe with the OCS, therefore the A/V Edge Server URI was not received	
Failure in initialization of SNMP agent.	
Fallback version is being used	Fallback version is being used. Restore current version. Version being used: [running version]; Current version: [current version].
Fan Problem Level Critical	
Fan Problem Level Major	
File error	 Possible reasons for the file error: XML file does not exist [file name]; Error no: [error number]. Not authorized to open XML file [file name]; Error no: [error number]. Unknown problem in opening XML file [file name]; Error no: [error number]. Failed to parse XML file [file name].
File system scan failure	File system scan failure: Failed to scan [file system path]. Multiple occurrences may point to a hardware problem. System is functioning.
File system space shortage	File system space shortage: Out of file system space in [file system path]; Free space: [free space percentage]% ([free space] Blocks) - Minimum free space required: [minimum free space percentage]% ([minimum free space] Blocks).
FIPS 140 failure	

FIPS 140 test result not received

Alarm Code	Alarm Description
Gatekeeper failure	Possible reasons for the Gatekeeper failure: Failed to register to alternate Gatekeeper. Gatekeeper discovery state Check GK IP address (GUI, ping) Gatekeeper DNS Host name not found. Gatekeeper Registration Timeout. Gatekeeper rejected GRQ due to invalid revision. Gatekeeper rejected GRQ due to resource unavailability. Gatekeeper rejected GRQ due to Terminal Exclusion. Gatekeeper rejected GRQ due to unsupported feature. Gatekeeper rejected GRQ due to Discovery Required. Gatekeeper rejected RRQ due to biscovery Required. Gatekeeper rejected RRQ due to biscovery Required. Gatekeeper rejected RRQ due to duplicate alias Check duplicate in aliases or in prefixes Gatekeeper rejected RRQ due to Generic Data. Gatekeeper rejected RRQ due to invalid alias. Gatekeeper rejected RRQ due to invalid call signaling address. Gatekeeper rejected RRQ due to invalid RAS address. Gatekeeper rejected RRQ due to invalid RAS address. Gatekeeper rejected RRQ due to invalid state. Gatekeeper rejected RRQ due to invalid state. Gatekeeper rejected RRQ due to invalid terminal alias. Gatekeeper rejected RRQ due to resource unavailability. Gatekeeper rejected RRQ due to Security Denial. Gatekeeper rejected RRQ due to to susupported Additive Registration. Gatekeeper rejected RRQ due to unsupported Palakeeper rejected RRQ due to unsupported Additive Registration. Gatekeeper rejected RRQ due to unsupported Additive Registration. Gatekeeper rejected RRQ due to unsupported Additive Registration. Gatekeeper rejected RRQ due to unsupported Transport. Gatekeeper rejected RRQ RRQ due to unsupported Requere. Gatekeeper rejected RRQ. Reason 18. Gatekeeper Unregistration State. Registration succeeded.
GUI System configuration file is invalid xml file	Check the Gatekeeper configuration. The XML format of the system configuration file that contains the user interface settings is invalid.
Hard disk error	Hard disk not responding.
Hot Backup: Master-Slave configuration conflict.	Possible reasons: • When both the MCUs are configured as Master or as Slave • The slave Collaboration Server is defined with the same IP as the Master.

Alarm Code	Alarm Description
Hot backup: Network issue	
Hot Backup: Paired MCU is unreachable.	
Initialization of ice stack failed	
Insufficient resources	The number of resources in the license is higher than the actual system resources. Check the media cards or insert a media card.
Insufficient UDP Ports	When defining fixed port, the number of defined UDP ports is lower than the required ports. Configure additional ports.
Internal System configuration during startup	System configuration during startup. Wait until Collaboration Server startup is completed.
Invalid System Configuration	
IP addresses of Signaling Host and Control Unit are the same	IP addresses of Signaling Host and Control Unit are identical. Assign different IP addresses to the Signaling Host and Control Unit.
IP Network Service added	
IP Network Service configuration modified	IP Network Service was modified. Reset the MCU.
IP Network Service deleted	IP Network Service was deleted. Reset the MCU.
IP Network Service not found	IP Service not found in the Network Services list. Configure the IP Network Service.
IPMC software upgrade in component	
IPS 140 test result not received	
ISDN/PSTN Network Services configuration changed	New ISDN/PSTN configuration. Reset the MCU for the change to take effect.
LDAP TLS: Failed to connect to OSCP responder	
Management Network not configured	Configure the Management Network.
Missing Central Signaling configuration	Configure the central signaling.
Missing Central Signaling IP configuration	
MPL startup failure. Authentication not received.	Authentication was not received from Switch. Check the switch card.

Alarm Code	Alarm Description
MPL startup failure. Management Network configuration not received.	Management Network message was not received. Check the Switch card.
Network interface is not configured. New interface need to be chosen	
Network traffic capture is on	
New certificate for CS need Collaboration Server reset to take effect	
No clock source	The system could not use any of the connected ISDN spans as clock source. Check the ISDN Settings.
No default ISDN/PSTN Network Service defined in ISDN/PSTN Network Services list	Set a default ISDN/PSTN Network Service.
No default IVR Service in IVR Services list	No default IVR Service in IVR Services list. Ensure that one conference IVR Service and one EQ IVR Service are set as default.
No IP Network Services defined	IP Network Service parameters missing. Configure the IP Network Service.
No ISDN/PSTN Network Services defined	No ISDN/PSTN Network Services were defined or no default ISDN/PSTN Network was defined.
No LAN connection	
No License for ISDN/PSTN. Please activate the RTM ISDN card through Polycom website	Configure the ISDN Network Service.
No response from Central Signaling	No connection with central signaling.
No response from RTM ISDN card	
No RTM-LAN or RTM-ISDN installed. One of these cards must be installed in the RealPresence Collaboration Server (RMX) 4000	
No usable unit for audio controller	No media card is installed, or the media card installed is not functioning. Install the appropriate media card.
OCS Registration failed	
Password expiration warning	
Please install a newer version	
Port configuration was modified	

Alarm Code	Alarm Description
Power off	
Power Problem Level Critical	
Power Problem Level Major	
Product activation failure	Assign a new activation key.
Product Type mismatch. System is restarting.	The user is alerted to a mismatch between the product type that is stored in MCU software and the product type received from another system component.
	In such a case the system is automatically restarted.
Received Notification failed	
Recording device has disconnected unexpectedly	
Red Alarm	When a certain timeout will be reached (after startup), MCMS will go over the configured Spans. A configured Span that is related to nonexistent card – will produce a 'RED_ALARM' Alert. Similarly on HotSwap: if an RTM card (or an MPM that has an RTM extension) is removed, MCMS will go over the configured Spans. A configured Span that is related to the removed card – will produce a 'RED_ALARM' Alert.
Requested changes to the certification repository were not completed. Repository must be updated to implement these changes.	
Resource process failed to request the Meeting Room list during startup.	Without the Meeting Rooms list, the system cannot allocate the appropriate dial numbers, Conference ID etc. and therefore cannot run conferences.
Restore Failed	Restoring the system configuration has failed as the system could not locate the configuration file in the selected path, or could not open the file.
Restore Succeeded	Restoring the system configuration has succeeded. Reset the MCU.
Restoring Factory Defaults. Default system settings will be restored once Reset is completed	Default system settings will be restored once Reset is completed.
Collaboration Server fails to connect to Active Directory server.	
Collaboration Server is uploading the version file. To cancel the upload and the upgrade, reset the Collaboration Server	
Collaboration Server user/password list will be reset	

Alarm Code	Alarm Description
RTM ISDN card not found	RTM ISDN card is missing. Install the RTM ISDN card.
RTM ISDN card startup procedure error	The RTM ISDN card cannot complete its startup procedure (usually after system reset). Check the card and/or reset the card.
Secured SIP communication failed	Error status (408) received from SIP proxy.
Security mode failed. Certificate has expired.	
Security mode failed. Certificate host name does not match the Collaboration Server host name.	
Security mode failed. Certificate is about to expire.	
Security mode failed. Certificate not yet valid.	
Security mode failed. Error in certificate file.	
Service Request failed	
SIP registrations limit reached	SIP registrations limit reached.
SIP TLS: Certificate has expired	The current TLS certificate files have expired and must be replaced with new files.
SIP TLS: Certificate is about to expire	The current TLS certificate files will expire shortly and will have to be replaced to ensure the communication with the OCS.
SIP TLS: Certificate subject name is not valid or DNS failed to resolve this name	This alarm is displayed if the name of the Collaboration Server in the certificate file is different from the FQDN name defined in the OCS.
SIP TLS: Failed to load or verify certificate files	This alarm indicates that the certificate files required for SIP TLS could not be loaded to the Collaboration Server. Possible causes are:
	 Incorrect certificate file name. Only files with the following names can be loaded to the system: rootCA.pem, pkey.pem, cert.pem and certPassword.txt
	 Wrong certificate file type. Only files of the following types can be loaded to the system: rootCA.pem, pkey.pem and cert.pem and certPassword.txt
	The contents of the certificate file does not match the system parameters
SIP TLS: Registration handshake failure	This alarm indicates a mismatch between the security protocols of the OCS and the Collaboration Server, preventing the Registration of the Collaboration Server to the OCS.

Alarm Code	Alarm Description
SIP TLS: Registration server not responding	 This alarm is displayed when the Collaboration Server does not receive a response from the OCS to the registration request in the expected time frame. Possible causes are: The Collaboration Server FQDN name is not defined in the OCS pool, or is defined incorrectly. The time frame for the expected response was too short and it will be updated with the next data refresh. The alarm may be cleared automatically the next time the data is refreshed. The Collaboration Server FQDN name is not defined in the DNS server. Ping the DNS using the Collaboration Server FQDN name to ensure that the Collaboration Server is correctly registered to the DNS.
SIP TLS: Registration transport error	This alarm indicates that the communication with the SIP server cannot be established. Possible causes are: Incorrect IP address of the SIP server The SIP server listening port is other than the one defined in the system The OCS services are stopped
Software upgrade in component	
SSH is enabled	
SWITCH not responding	Check the Switch card.
System Cards MPM Plus mode are not supported in Event mode	
System configuration changed. Please reset the MCU	
System Configuration modified	System configuration flags were modified. Reset the MCU.
System resources of Audio ports usage has exceeded Port Gauge threshold	
System resources of Video ports usage has exceeded Port Gauge threshold	
System resources usage has exceeded Port Gauge threshold	
Temperature Level - Critical	Possible explanations: • Temperature has reached a critical level. Card or if critical system element the MCU will shut down.
Temperature Level - Major	Possible explanations: • Temperature has reached a problematic level and requires attention.

Alarm Code	Alarm Description
The Log file system is disabled because of high system CPU usage	
The MCCF channel is not connected	
The software contains patch(es)	The software contains patch(es).
The system has been configured for Ultra Secure Mode, but communication is not secured until a TLS certificate is installed and the MCU is set to Secured Communication.	Although the System Flag ULTRA_SECURE_MODE is set to YES, the Ultra Secure Mode is not fully implemented as the TLS certificate was not installed. Please install the TLS certificate and set the MCU to Secured Communication Mode to fully enable the Enhanced Security Environment.
Unable to connect to Exchange Server.	
User Name SUPPORT cannot be used in Enhanced Security Mode	
Version upgrade is in progress	
Voltage problem	Possible reasons for the problem: Card voltage problem. Shelf voltage problem. Voltage problem
Warning: Upgrade started and SAFE Upgrade protection is turned OFF	
Yellow Alarm	Problem sending/receiving data from/to network. Check the cables.

Appendix C - CDR Fields, Unformatted File

The CDR (Call Detail Records) utility is used to retrieve conference information to a file. The CDR utility can retrieve conference information to a file in both formatted and unformatted formats.

Unformatted CDR files contain multiple records. The first record in each file contains information about the conference in general, such as the conference name and start time. The remaining records each contain information about one event that occurred during the conference, such as a participant connecting to the conference, or a user extending the length of the conference. The first field in each record identifies the event type, and this is followed by values containing information about the event. The fields are separated by commas.

Formatted files contain basically the same information as unformatted files, but with the field values replaced by descriptions. Formatted files are divided into sections, each containing information about one conference event. The first line in each section is a title describing the type of event, and this is followed by multiple lines, each containing information about the event in the form of a descriptive field name and value.



The field names and values in the formatted file will appear in the language being used for the *Collaboration Server Web Client* user interface at the time when the CDR information is retrieved. The value of the fields that support Unicode values, such as the info fields, will be stored in the CDR file in UTF8. The application that reads the CDR file must support Unicode.

The MCU sends the entire CDR file via API or HTTP, and the Collaboration Server or external application does the processing and sorting. The Collaboration Server ignores events that it does not recognize, that is, events written in a higher version that do not exist in the current version. Therefore, to enable compatibility between versions, instead of adding new fields to existing events, new fields are added as separate events, so as not to affect the events from older versions. This allows users with lower versions to retrieve CDR files that were created in higher versions.



This appendix describes the fields and values in the unformatted CDR records.

Although the formatted files contain basically the same information, in a few instances a single field in the unformatted file is converted to multiple lines in the formatted file, and in other cases, multiple fields in the unformatted file are combined into one line in the formatted file.

In addition, to enable compatibility for applications that were written for the MGC family, the unformatted file contains fields that were supported by the MGC family, but are not supported by the Collaboration Server, whereas these fields are omitted from the formatted file.



The following features are not supported with Collaboration Server 1800:

- ISDN/PSTN connections
- Video Switching Conferences
- · Gateway Calls

Any reference to these features relates to the RealPresence® Collaboration Server 1500/2000/4000.

The Conference Summary Record

The conference summary record (the first record in the unformatted CDR file) contains the following fields

:Conference Summary Record Fields

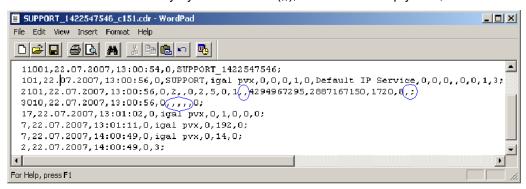
Field	Description
File Version	The version of the CDR utility that created the file.
Conference Routing Name	The Routing Name of the conference.
Internal Conference ID	The conference identification number as assigned by the system.
Reserved Start Time	The time the conference was scheduled to start in Greenwich Mean Time (GMT). The reservation time of a reservation that was started immediately or of an ongoing conference is the same as the <i>Actual Start Time</i> .
Reserved Duration	The amount of time the conference was scheduled to last.
Actual Start Time	The actual time the conference started in GMT.
Actual Duration	The actual conference duration.
Status	The conference status code as follows: 1 - The conference is an ongoing conference. 2 - The conference was terminated by a user. 3 - The conference ended at the scheduled end time. 4 - The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. 5 - The conference never started. 6 - The conference could not start due to a problem. 8 - An unknown error occurred. 9 - The conference was terminated by a participant using DTMF codes. Note: If the conference was terminated by an MCU reset, this field will contain the value 1 (ongoing conference).
File Name	The name of the conference log file.
GMT Offset Sign	Indicates whether the <i>GMT Offset</i> is positive or negative. The possible values are: 0 - Offset is negative. GMT Offset will be subtracted from the GMT Time. 1 - Offset is positive. GMT Offset will be added to the GMT Time.

Field	Description
GMT Offset	The time zone difference between Greenwich and the Collaboration Server's physical location in hours and minutes.
	Together with the <i>GMT Offset Sign</i> field the <i>GMT Offset</i> field is used to define the Collaboration Server local time. For example, if the <i>GMT Offset Sign</i> is 0 and <i>GMT Offset</i> is 3 hours then the time zone of the Collaboration Server's physical location is -3, which will be subtracted from the GMT time to determine the local time. However, if the <i>GMT Offset Sign</i> is 1 and <i>GMT Offset</i> is 4 hours then the time zone of the Collaboration Server's physical location is +4, which will be added to the GMT time to determine the local time.
File Retrieved	Indicates if the file has been retrieved and saved to a formatted file, as follows: 0 - No 1 - Yes

Event Records

The event records, that is, all records in the unformatted file except the first record, contain standard fields, such as the event type code and the time stamp, followed by fields that are event specific.

The event fields are separated by commas. Two consecutive commas with nothing between them (,,), or a comma followed immediately by a semi-colon (,;), indicates an empty field, as in the example below:



Standard Event Record Fields

All event records start with the following fields:

- The CDR event type code. For a list of event type codes and descriptions, refer to CDR Event Types.
- · The event date.
- The event time.
- The structure length. This field is required for compatibility purposes, and always contains the value
 0.

Event Types

The table below contains a list of the events that can be logged in the CDR file, and indicates where to find details of the fields that are specific to that type of event.



The event code identifies the event in the unformatted CDR file, and the event name identifies the event in the formatted CDR file.

CDR Event Types

Event Code	Event Name	Description
1	CONFERENCE START	The conference started. For more information about the fields, see Event Fields for Event 1 - CONFERENCE START. Note: There is one CONFERENCE START event per conference. It is always the first event in the file, after the conference summary record. It contains conference details, but not participant details.
2	CONFERENCE END	The conference ended. For more information about the fields, see Event Fields for Event 2 - CONFERENCE END. Note: There is one CONFERENCE END event per conference, and it is always the last event in the file.
3	ISDN/PSTN CHANNEL CONNECTED	An ISDN/PSTN channel connected. For more information about the fields, see Event fields for Event 3 - ISDN/PSTN CHANNEL CONNECTED.
4	ISDN/PSTN CHANNEL DISCONNECTED	An ISDN/PSTN channel disconnected. For more information about the fields, see Event fields for Event 4 - ISDN/PSTN CHANNEL DISCONNECTED.
5	ISDN/PSTN PARTICIPANT CONNECTED	An ISDN/PSTN participant connected to the conference. For more information about the fields, see Event fields for Event 5 - ISDN/PSTN PARTICIPANT CONNECTED.
7	PARTICIPANT DISCONNECTED	A participant disconnected from the conference. For more information about the fields, see Event Fields for Event 7 - PARTICIPANT DISCONNECTED.
10	DEFINED PARTICIPANT	Information about a defined participant, that is, a participant who was added to the conference before the conference started. For more information about the fields, see Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT. Note: There is one event for each participant defined before the conference started.

Event Code	Event Name	Description
15	H323 CALL SETUP	Information about the IP address of the participant. For more information about the fields, see Event fields for Event 15 - H323 CALL SETUP.
17	H323 PARTICIPANT CONNECTED	An H.323 participant connected to the conference. For more information about the fields, see Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED.
18	NEW UNDEFINED PARTICIPANT	A new undefined participant joined the conference. For more information about the fields, see Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT.
20	BILLING CODE	A billing code was entered by a participant using DTMF codes. For more information about the fields, see Event Fields for Event 20 - BILLING CODE.
21	SET PARTICIPANT DISPLAY NAME	A user assigned a new name to a participant, or an end point sent its name. For more information about the fields, see Event Fields for Event 21 - SET PARTICIPANT DISPLAY NAME.
22	DTMF CODE FAILURE	An error occurred when a participant entered a DTMF code. For more information about the fields, see Event Fields for Event 22 - DTMF CODE FAILURE.
23	SIP PARTICIPANT CONNECTED	A SIP participant connected to the conference. For more information about the fields, see Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED.
26	RECORDING LINK	A recording event, such as recording started or recording resumed, occurred. For more information about the fields, see Event fields for Event 26 - RECORDING LINK.
28	SIP PRIVATE EXTENSIONS	Contains SIP Private Extensions information. For more information about the fields, see Event Fields for Event 28 - SIP PRIVATE EXTENSIONS.
30	GATEKEEPER INFORMATION	Contains the gatekeeper caller ID, which makes it possible to match the CDR in the gatekeeper and in the MCU. For more information about the fields, see Event Fields for Event 30 - GATEKEEPER INFORMATION.
31	PARTICIPANT CONNECTION RATE	Information about the line rate of the participant connection. This event is added to the CDR file each time the endpoint changes its connection bit rate. For more information about the fields, see Event fields for Event 31 - PARTICIPANT CONNECTION RATE.
32	EVENT NEW UNDEFINED PARTY CONTINUE IPV6 ADDRESS	Information about the IPv6 address of the participant's endpoint.

Event Code	Event Name	Description
33	PARTY CHAIR UPDATE	Participants connect to the conferences as standard participants and they are designated as chairpersons either by entering the chairperson password during the IVR session upon connection, or while participating in the conference using the appropriate DTM code. For more information about the fields, see Event fields for Event 33 - PARTY CHAIR UPDATE.
34	PARTICIPANT MAXIMUM USAGE INFORMATION	This event includes information of the maximum line rate, maximum resolution and maximum frame rate used by H.323 or SIP participant during the conference.
35	SVC SIP PARTICIPANT CONNECTED	An SVC user connected over SIP. For more information about the fields, see Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED.
100	USER TERMINATE CONFERENCE	A user terminated the conference. For more information about the fields, see Event Fields for Event 100 - USER TERMINATE CONFERENCE.
101	USER ADD PARTICIPANT	A user added a participant to the conference during the conference. For more information about the fields, see Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT.
102	USER DELETE PARTICIPANT	A user deleted a participant from the conference. For more information about the fields, see Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT.
103	USER DISCONNECT PARTICIPANT	A user disconnected a participant. For more information about the fields, see Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT.
104	USER RECONNECT PARTICIPANT	A user reconnected a participant who was disconnected from the conference. For more information about the fields, see Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT.
105	USER UPDATE PARTICIPANT	A user updated the properties of a participant during the conference. For more information about the fields, see Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT.
106	USER SET END TIME	A user modified the conference end time. For more information about the fields, see Event Fields for Event 106 - USER SET END TIME.

Event Code	Event Name	Description
107	OPERATOR MOVE PARTY FROM CONFERENCE	The participant moved from an Entry Queue to the destination conference or between conferences. For more information about the fields, see Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY.
108	OPERATOR MOVE PARTY TO CONFERENCE	The Collaboration Server User moved the participant from an ongoing conference to another conference. For more information, see Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE.
109	OPERATOR ATTEND PARTY	The Collaboration Server User moved the participant to the Operator conference. For more information, see Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY.
111	OPERATOR BACK TO CONFERENCE PARTY	The Collaboration Server User moved the participant back to his Home (source) conference. For more information, see Event Fields for Event 111 - OPERATOR BACK TO CONFERENCE PARTY.
112	OPERATOR ATTEND PARTY TO CONFERENCE	The Collaboration Server User moved the participant from the Operator conference to another conference. For more information, see Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE.
1001	NEW UNDEFINED PARTICIPANT CONTINUE 1	Additional information about a NEW UNDEFINED PARTICIPANT event. For more information about the fields, see Event Fields for Event 1001 - NEW UNDEFINED PARTY CONTINUE 1.
2001	CONFERENCE START CONTINUE 1	Additional information about a CONFERENCE START event. For more information about the fields, see Event Fields for Event 2001 - CONFERENCE START CONTINUE 1.
2007	PARTICIPANT DISCONNECTED CONTINUE 1	Additional information about a PARTICIPANT DISCONNECTED event. For more information about the fields, see Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1.
2010	DEFINED PARTICIPANT CONTINUE 1	Additional information about a DEFINED PARTICIPANT event. For more information about the fields, see Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1.
2011	RESERVED PARTICIPANT CONTINUE PV6 ADDRESS	Additional information about a DEFINED PARTICIPANT event that includes the IPv6 addressing of the defined participant. For more details, see Event Fields for Events 2011, 2012, and 2016.

Event Code	Event Name	Description
2012	RESERVED PARTICIPANT CONTINUE 2	Additional information about a DEFINED PARTICIPANT event. For more information about the fields, see Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2.
2101	USER ADD PARTICIPANT CONTINUE 1	Additional information about a USER ADD PARTICIPANT event. For more information about the fields, see Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1.
2102	USER ADD PARTICIPANT CONTINUE 2	Additional information about a USER ADD PARTICIPANT event. For more information about the fields, see Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2.
2105	USER UPDATE PARTICIPANT CONTINUE 1	Additional information about a USER UPDATE PARTICIPANT event. For more information about the fields, see Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1.
2106	USER UPDATE PARTICIPANT CONTINUE 2	Additional information about a USER UPDATE PARTICIPANT event. For more information about the fields, see Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2.
3010	PARTICIPANT INFORMATION	The contents of the participant information fields. For more information about the fields, see Event Fields for Event 3010 - PARTICIPANT INFORMATION.
5001	CONFERENCE START CONTINUE 4	Additional information about a CONFERENCE START event. For more information about the fields, see Event Fields for Event 5001 - CONFERENCE START CONTINUE 4. Note: An additional CONFERENCE START CONTINUE 4 event will be written to the CDR each time the value of one of the following conference fields is modified: Conference Password Chairperson Password Info1, Info2 or Info3 Billing Info These additional events will only contain the value of the modified field.
6001	CONFERENCE START CONTINUE 5	Additional information about a CONFERENCE START event. For more information about the fields, see Event Fields for Event 6001 - CONFERENCE START CONTINUE 5.

Event Code	Event Name	Description
11001	CONFERENCE START CONTINUE 10	Additional information about a CONFERENCE START event. This event contains the Display Name. For more information about the fields, see Event Fields for Event 11001 - CONFERENCE START CONTINUE 10.



This list only includes events that are supported by the Collaboration Server. For a list of MGC Manager events that are not supported by the Collaboration Server, see MGC Manager Events that are not Supported by the Collaboration Server.

Event Specific Fields

The following tables describe the fields which are specific to each type of event.



Some fields that were supported by the MGC Manager, are not supported by the Collaboration Server. In addition, for some fields the Collaboration Server has a fixed value, whereas the MGC Manager supported multiple values. For more information about the MGC Manager fields and values, see the MGC Manager User's Guide Volume II, Appendix A.

Event Fields for Event 1 - CONFERENCE START

Field	Description
Dial-Out Manually Indicates whether the conference was a dial-out manually conference or not. Currently the only value is:	
	0 - The conference was not a dial-out manually conference, that is, the MCU initiates the communication with dial-out participants, and the user does not need to connect them manually.
Auto Terminate	Indicates whether the conference was set to end automatically if no participant joins the conference for a predefined time period after the conference starts, or if all participants disconnect from the conference and the conference is empty for a predefined time period. Possible values are:
	0 - The conference was not set to end automatically.
	1 - The conference was set to end automatically.

Field	Description
Line Rate	The conference line rate, as follows: 0 - 64 kbps 6 - 384 kbps 12 - 1920 kbps 13 - 128 kbps 15 - 256 kbps 23 - 512 kbps 24 - 768 kbps 26 - 1152 kbps 29 - 1472 kbps 32 - 96 kbps
Line Rate (cont.)	33 - 1024 kbps 34 - 4096 kbps
Restrict Mode	Not supported. Always contains the value 0 .
Audio Algorithm	The audio algorithm. Currently the only value is: 255 - Auto
Video Session	The video session type. Currently the only value is: 3 - Continuous Presence
Video Format	The video format. Currently the only value is: 255 - Auto
CIF Frame Rate	The CIF frame rate. Currently the only value is: 255 -Auto
QCIF Frame Rate	The QCIF frame rate: Currently the only value is: 255 - Auto
LSD Rate	Not supported. Always contains the value 0 .
HSD Rate	Not supported. Always contains the value 0 .
T120 Rate	Not supported. Always contains the value 0 .

Event Fields for Event 2001 - CONFERENCE START CONTINUE 1

Field	Description
Audio Tones	Not supported. Always contains the value 0 .
Alert Tone	Not supported. Always contains the value 0 .
Talk Hold Time	The minimum time that a speaker has to speak to become the video source. The value is in units of 0.01 seconds. Currently the only value is 150 , which indicates a talk hold time of 1.5 seconds.
Audio Mix Depth	The maximum number of participants whose audio can be mixed. Currently the only value is 5 .
Operator Conference	Not supported. Always contains the value 0 .
Video Protocol	The video protocol. Currently the only value is: 255 - Auto
Meet Me Per Conference	Indicates the Meet Me Per Conference setting. Currently the only value is: 1 - The Meet Me Per Conference option is enabled, and dial-in participants can join the conference by dialing the dial-in number.
Number of Network Services	Not supported. Always contains the value 0 .
Chairperson Password	The chairperson password for the conference. An empty field "" means that no chairperson password was assigned to the conference.
Chair Mode	Not supported. Always contains the value 0 .
Cascade Mode	The cascading mode. Currently the only value is: 0 - None
Master Name	Not supported. This field remains empty.
Minimum Number of Participants	The number of participants for which the system reserved resources. Additional participants may join the conference without prior reservation until all the resources are utilized. Currently the only value is 0 .
Allow Undefined Participants	Indicates whether or not undefined dial-in participants can connect to the conference. Currently the only value is: 1 - Undefined participants can connect to the conference

Field	Description
Time Before First Participant Joins	Note: This field is only relevant if the Auto Terminate option is enabled. Indicates the number of minutes that should elapse from the time the conference starts, without any participant connecting to the conference, before the conference is automatically terminated by the MCU.
Time After Last Participant Quits	Note: This field is only relevant if the Auto Terminate option is enabled. Indicates the number of minutes that should elapse after the last participant has disconnected from the conference, before the conference is automatically terminated by the MCU.
Conference Lock Flag	Not supported. Always contains the value 0 .
Maximum Number of Participants	The maximum number of participants that can connect to the conference at one time. The value 65535 (auto) indicates that as many participants as the MCU's resources allow can connect to the conference, up to the maximum possible for the type of conference.
Audio Board ID	Not supported. Always contains the value 65535 .
Audio Unit ID	Not supported. Always contains the value 65535 .
Video Board ID	Not supported. Always contains the value 65535 .
Video Unit ID	Not supported. Always contains the value 65535 .
Data Board ID	Not supported. Always contains the value 65535 .
Data Unit ID	Not supported. Always contains the value 65535 .
Message Service Type	The Message Service type. Currently the only value is: 3 - IVR
Conference IVR Service	The name of the IVR Service assigned to the conference. Note: If the name of the IVR Service contains more than 20 characters, it will be truncated to 20 characters.
Lecture Mode Type	Indicates the type of Lecture Mode, as follows: 0 - None 1 - Lecture Mode 3 - Presentation Mode
Lecturer	Note: This field is only relevant if the Lecture Mode Type is Lecture Mode. The name of the participant selected as the conference lecturer.

Field	Description
Time Interval	Note: This field is only relevant if Lecturer View Switching is enabled. The number of seconds a participant is to be displayed in the lecturer window before switching to the next participant. Currently the only value is 15.
Lecturer View Switching	Note: This field is only relevant when Lecture Mode is enabled. Indicates the lecturer view switching setting, as follows: 0 - Automatic switching between participants is disabled. 1 - Automatic switching between participants is enabled.
Audio Activated	Not supported. Always contains the value 0 .
Lecturer ID	Not supported. Always contains the value 4294967295 .

Event Fields for Event 5001 - CONFERENCE START CONTINUE 4

Field	Description	
Note: When this event occurs as the result of a change to the value of one of the event fields, the event will only contain the value of the modified field. All other fields will be empty.		
Conference ID	The conference ID.	
Conference Password	The conference password. An empty field "" means that no conference password was assigned to the conference.	
Chairperson Password	The chairperson password. An empty field "" means that no chairperson password was assigned to the conference.	
Info1	The contents of the conference information fields.	
Info2	These fields enable users to enter general information for the conference, such as the	
Info3	company name, and the contact person's name and telephone number.	
	The maximum length of each field is 80 characters.	
Billing Info	The billing code.	

Event Fields for Event 6001 - CONFERENCE START CONTINUE 5

Field	Description
Encryption	Indicates the conference encryption setting, as follows: 0 - The conference is <i>not</i> encrypted. 1 - The conference is encrypted.

Event Fields for Event 11001 - CONFERENCE START CONTINUE 10

Field	Description
Display Name	The Display Name of the conference.

Event Fields for Event 2 - CONFERENCE END

Field	Description
Conference End Cause	Indicates the reason for the termination of the conference, as follows: 1 - The conference is an ongoing conference or the conference was terminated by an MCU reset. 2 - The conference was terminated by a user. 3 - The conference ended at the scheduled end time. 4 - The conference ended automatically because no participants joined the conference for a predefined time period, or all the participants disconnected from the conference and the conference was empty for a predefined time period. 5 - The conference never started. 6 - The conference could not start due to a problem. 8 - An unknown error occurred. 9 - The conference was terminated by a participant using DTMF codes.

Event fields for Event 3 - ISDN/PSTN CHANNEL CONNECTED

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Channel ID	The channel identifier.
Number of Channels	The number of channels being connected for this participant.
Connect Initiator	Indicates who initiated the connection, as follows: 0 - Collaboration Server 1 - Participant Any other number - Unknown
Call Type	The call type, as follows: 68 - 56 KBS data call 72 - 1536kbs data call (PRI only) 75 - 56 KBS data call 77 - Modem data service 79 - 384kbs data call (PRI only) 86 - Normal voice call

Field	Description
Network Service Program	The Network Service program, as follows: 0 - None 1 - ATT_SDN or NTI_PRIVATE 3 - ATT_MEGACOM or NTI_OUTWATS 4 - NTI FX 5 - NTI TIE TRUNK 6 - ATT ACCUNET 8 - ATT 1800 16 - NTI_TRO
Preferred Mode	The value of the preferred/exclusive field for B channel selection (the PRF mode), as follows: 0 - None 1 - Preferred 2 - Exclusive For more details refer to the Q.931 standard.
Calling Participant Number Type	The type of calling number, as follows: 0 - Unknown, default 1 - International 2 - National 3 - Network specific 4 - Subscriber 6 - Abbreviated
Calling Participant Number Plan	The calling participant number plan. 0 - Unknown 1 - ISDN/PSTN 9 - Private
Calling Participant Presentation Indicator	The calling participant presentation indicator, as follows: 0 - Presentation allowed, default 1 - Presentation restricted 2 - Number not available 255 - Unknown
Calling Participant Screening Indicator	The calling participant screening indicator, as follows: 0 - Participant not screened, default 1 - Participant verification succeeded 2 - Participant verification failed 3 - Network provided 255 - Unknown
Calling Participant Phone Number	The telephone number used for dial-in.

Field	Description
Called Participant Number Type	The type of number called, as follows: 0 - Unknown, default 1 - International 2 - National 3 - Network specific 4 - Subscriber 6 - Abbreviated
Called Participant Number Plan	The called participant number plan, as follows: 0 - Unknown 1 - ISDN/PSTN 9 - Private
Called Participant Phone Number	The telephone number used for dial-out.

Event fields for Event 4 - ISDN/PSTN CHANNEL DISCONNECTED

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.
Channel ID	The channel identifier.
Disconnect Initiator	Indicates who initiated the disconnection, as follows: 0 - Collaboration Server 1 - Participant Any other number - Unknown
Disconnect Coding Standard	The disconnection cause code standard. For values and explanations, see the Q.931 Standard.
Disconnect Location	The disconnection cause location. For values and explanations, see the Q.931 Standard.
Q931 Disconnection Cause	The disconnection cause value. For values and explanations, see the Q.931 Standard.

Event fields for Event 5 - ISDN/PSTN PARTICIPANT CONNECTED

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Field	Description
Participant Status	The participant status, as follows:
	0 - Idle
	1 - Connected
	2 - Disconnected
	3 - Waiting for dial-in
	4 - Connecting
	5 - Disconnecting
	6 - Partially connected. Party has completed H.221 capability exchange
	7 - Deleted by a user
	8 - Secondary. The participant could not connect the video channels and is connected via audio only
	10 - Connected with problem
	11 - Redialing
Remote	Note: This field is only relevant to ISDN video participants.
Capabilities	The remote capabilities in H.221 format.
Remote	Note: This field is only relevant to ISDN video participants.
Communication Mode	The remote communication mode in H.221 format.
Secondary Cause	Note: This field is only relevant to ISDN video participants and only if the Participant Status is Secondary.
	The cause for the secondary connection (not being able to connect the video channels), as follows:
	0 - Default
	11 - The incoming video parameters are not compatible with the conference video parameters
	12 - H.323 card failure
	13 - The conference video settings are not compatible with the endpoint capabilities
	14 - The new conference settings are not compatible with the endpoint capabilities
Secondary Cause	15 - Video stream violation due to incompatible annexes or other discrepancy.
(cont.)	16 - Inadequate video resources
	17 - When moved to a Transcoding or Video Switching conference, the participant's video capabilities are not supported by the video cards
	18 - Video connection could not be established
	24 - The endpoint closed its video channels
	25 - The participant video settings are not compatible with the conference protocol
	26 - The endpoint could not re-open the video channel after the conference video mode was changed
	27 - The gatekeeper approved a lower bandwidth than requested
	28 - Video connection for the SIP participant is temporarily unavailable
	29 - AVF problem. Insufficient bandwidth.
	30 - H2.39 bandwidth mismatch
	255 - Other

Event Fields for Event 7 - PARTICIPANT DISCONNECTED

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Call Disconnection Cause	The disconnection cause. For more information about possible values, see Disconnection Cause Values.
Q931 Disconnect Cause	If the disconnection cause is "No Network Connection" or "Participant Hang Up", then this field indicates the Q931 disconnect cause.

Event Fields for Event 2007 - PARTICIPANT DISCONNECTED CONTINUE 1

Field	Description
Rx Synchronization Loss	The number of times that the general synchronization of the MCU was lost.
Tx Synchronization Loss	The number of times that the general synchronization of the participant was lost.
Rx Video Synchronization Loss	The number of times that the synchronization of the MCU video unit was lost.
Tx Video Synchronization Loss	The number of times that the synchronization of the participant video was lost.
Mux Board ID	Not supported. Always contains the value 0 .
Mux Unit ID	Not supported. Always contains the value 0 .
Audio Codec Board ID	Not supported. Always contains the value 0 .
Audio Codec Unit ID	Not supported. Always contains the value 0 .
Audio Bridge Board ID	Not supported. Always contains the value 0 .
Audio Bridge Unit ID	Not supported. Always contains the value 0 .
Video Board ID	Not supported. Always contains the value 0 .
Video Unit ID	Not supported. Always contains the value 0 .

Field	Description
T.120 Board ID	Not supported. Always contains the value 0 .
T.120 Unit ID	Not supported. Always contains the value 0 .
T.120 MCS Board ID	Not supported. Always contains the value 0 .
T.120 MCS Unit ID	Not supported. Always contains the value 0 .
H.323 Board ID	Not supported. Always contains the value 0 .
H323 Unit ID	Not supported. Always contains the value 0 .

Event Fields for Events 10, 101, 105 - DEFINED PARTICIPANT, USER ADD PARTICIPANT, USER UPDATE PARTICIPANT

Field	Description
User Name	The login name of the user who added the participant to the conference, or updated the participant properties.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Dialing Direction	The dialing direction, as follows: 0 - Dial-out 5 - Dial-in
Bonding Mode	Not supported. Always contains the value 0 .
Number Of Channels	Note: This field is only relevant to ISDN/PSTN participants. The number of channels being connected for this participant.
Net Channel Width	Not supported. Always contains the value 0 .
Network Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Not supported. Always contains the value 0 .

Field	Description
Audio Only	Indicates the participant's Audio Only setting, as follows: 0 - The participant is <i>not</i> an Audio Only participant 1 - The participant is an Audio Only participant 255 - Unknown
Default Number Type	Note: This field is only relevant to ISDN/PSTN participants. The type of telephone number, as follows: 0 - Unknown 1 - International 2 - National 3 - Network specific 4 - Subscriber 6 - Abbreviated 255 - Taken from Network Service, default Note: For dial-in participants, the only possible value is: 255 - Taken from Network Service
Net Sub-Service Name	Not supported. This field remains empty.
Number of Participant Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. The number of participant phone numbers. In a dial-in connection, the participant phone number is the CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, participant phone numbers are the phone numbers dialed by the MCU for each participant channel.
Number of MCU Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. The number of MCU phone numbers. In a dial-in connection, the MCU phone number is the number dialed by the participant to connect to the MCU. In a dial-out connection, the MCU phone number is the MCU (CLI) number as seen by the participant.
Party and MCU Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. No, one or more fields, one field for each participant and MCU phone number. The participant phone numbers are listed first, followed by the MCU phone numbers.
Identification Method	Note: This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: 1 - Called phone number, IP address or alias 2 - Calling phone number, IP address or alias
Meet Me Method	Note: This field is only relevant to dial-in participants. The meet-me per method. Currently the only value is: 3 - Meet-me per participant

Event Fields for Events 2010, 2011, 2015 - DEFINED PARTICIPANT CONTINUE 1, USER ADD PARTICIPANT CONTINUE 1, USER UPDATE PARTICIPANT CONTINUE 1

Field	Description
Network Type	The type of network between the participant and the MCU, as follows: 0 - ISDN/PSTN 2 - H.323 5 - SIP
H.243 Password	Not supported. This field remains empty.
Chair	Not supported. Always contains the value 0 .
Video Protocol	The video protocol used by the participant, as follows: 1 - H.261 2 - H.263 4 - H.264 255 - Auto
Broadcasting Volume	The broadcasting volume assigned to the participant. The value is between 1 (lowest) and 10 (loudest). Each unit movement increases or decreases the volume by 3 dB.
Undefined Participant	Indicates whether are not the participant is an undefined participant, as follows: 0 - The participant is <i>not</i> an undefined participant. 2 - The participant is an undefined participant.
Node Type	The node type, as follows: 0 - MCU 1 - Terminal
Bonding Phone Number	Note: This field is only relevant to ISDN/PSTN participants. The phone number for Bonding dial-out calls. Bonding is a communication protocol that aggregates from two up to thirty 64 Kbps B channels together, to look like one large bandwidth channel.
Video Bit Rate	The video bit rate in units of kilobits per second. A value of 4294967295 denotes auto, and in this case, the rate is computed by the MCU.
IP Address	Note: This field is only relevant to IP participants. The IP address of the participant. An address of 4294967295 indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Signaling Port	Note: This field is only relevant to IP participants. The signaling port used for participant connection.

Field	Description
H.323 Participant Alias Type/SIP Participant Address Type	Note: This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: 7 - E164 8 - H.323 ID 13 - Email ID 14 - Participant number For SIP participants, the address type, as follows: 1 - SIP URI 2 - Tel URL
H.323 Participant Alias Name/SIP Participant Address	Note: This field is only relevant to IP participants. For H.323 participants: The participant alias. The alias may contain up to 512 characters. For SIP participants: The participant address. The address may contain up to 80 characters.

Event Fields for Event 2011 - DEFINED PARTICIPANT CONTINUE 2, Event 2012 - USER ADD PARTICIPANT CONTINUE 2, Event 2016 - USER UPDATE PARTICIPANT CONTINUE 2

Field	Description
Encryption	Indicates the participant's encryption setting as follows: 0 - The participant is <i>not</i> encrypted. 1 - The participant is encrypted. 2 - Auto. The conference encryption setting is applied to the participant.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Event fields for Event 15 - H323 CALL SETUP

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Connect Initiator	Indicates who initiated the connection, as follows: 0 - MCU 1 - Remote participant Any other number - Unknown

Field	Description
Min Rate	The minimum line rate used by the participant. The data in this field should be ignored. For accurate rate information, see CDR event 31.
Max Rate	The maximum line rate achieved by the participant. The data in this field should be ignored. For accurate rate information, see CDR event 31.
Source Party Address	The IP address of the calling participant. A string of up to 255 characters.
Destination Party Address	The IP address of the called participant. A string of up to 255 characters.
Endpoint Type	The endpoint type, as follows: 0 - Terminal 1 - Gateway 2 - MCU 3 - Gatekeeper 4 - Undefined

Event Fields for Events 17, 23 - H323 PARTICIPANT CONNECTED, SIP PARTICIPANT CONNECTED

Field	Description
Participant Name	The name of the participant.
	An empty field "" denotes an unidentified participant or a participant whose name is unspecified.
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows:
	0 - Idle
	1 - Connected
	2 - Disconnected
	3 - Waiting for dial-in
	4 – Connecting
	5 - Disconnecting
	6 - Partially connected. Party has completed H.221 capability exchange
	7 - Deleted by a user
	8 - Secondary. The participant could not connect the video channels and is connected via audio only
	10 - Connected with problem
	11 - Redialing
Capabilities	Not supported.
	Always contains the value 0 .
Remote	Not supported.
Communication Mode	Always contains the value 0 .

Field	Description
Secondary Cause	Note: This field is only relevant if the Participant Status is Secondary.
	The cause for the secondary connection (not being able to connect the video channels), as follows:
	0 - Default
	11 - The incoming video parameters are not compatible with the conference video parameters
	13 - The conference video settings are not compatible with the endpoint capabilities
	14 - The new conference settings are not compatible with the endpoint capabilities
	15 - Video stream violation due to incompatible annexes or other discrepancy
	16 - Inadequate video resources
	17 - When moved to a Transcoding or Video Switching conference, the participant's video capabilities are not supported by the video cards
	18 - Video connection could not be established
	24 - The endpoint closed its video channels
	25 - The participant video settings are not compatible with the conference protocol
	26 - The endpoint could not re-open the video channel after the conference video mode was changed
	27 - The gatekeeper approved a lower bandwidth than requested
	28 - Video connection for the SIP participant is temporarily unavailable
	255 - Other

Event Fields for Event 18 - NEW UNDEFINED PARTICIPANT

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Dialing Direction	The dialing direction, as follows 0 - Dial-out 5 - Dial-in
Bonding Mode	Not supported. Always contains the value 0 .
Number of Channels	Note: This field is only relevant to ISDN/PSTN participants. The number of channels being connected for this participant.
Net Channel Width	Not supported. Always contains the value 0 .
Network Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Not supported. Always contains the value 0 .

Field	Description
Audio Only	Indicates the participant's Audio Only setting, as follows: 0 - The participant is <i>not</i> an Audio Only participant 1 - The participant is an Audio Only participant 255 - Unknown
Default Number Type	Note: This field is only relevant to ISDN/PSTN participants. The type of telephone number. Note: Since undefined participants are always dial-in participants, the only possible value is: 255 - Taken from Network Service
Net Sub-Service Name	Not supported. This field remains empty.
Number of Participant Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. The number of participant phone numbers. The participant phone number is the CLI (Calling Line Identification) as identified by the MCU.
Number of MCU Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. The number of MCU phone numbers. The MCU phone number is the number dialed by the participant to connect to the MCU.
Party and MCU Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. No, one or more fields, one field for each participant and MCU phone number. The participant phone numbers are listed first, followed by the MCU phone numbers.
Identification Method	Note: This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: 1 - Called phone number, IP address or alias 2 - Calling phone number, IP address or alias
Meet Me Method	Note: This field is only relevant to dial-in participants. The meet-me per method, as follows: 3 - Meet-me per participant
Network Type	The type of network between the participant and the MCU, as follows: 0 - ISDN/PSTN 2 - H.323 5 - SIP
H.243 Password	Not supported. This field remains empty.
Chair	Not supported. Always contains the value 0 .
Video Protocol	The video protocol, as follows: 1 - H.261 2 - H.263 4 - H.264 255 - Auto

Field	Description
Broadcasting Volume	The broadcasting volume assigned to the participant. The value is between 1 (lowest) and 10 (loudest). Each unit movement increases or decreases the volume by 3 dB.
Undefined Participant	Indicates whether are not the participant is an undefined participant, as follows: 0 - The participant is <i>not</i> an undefined participant. 2 - The participant is an undefined participant.
Node Type	The node type, as follows: 0 - MCU 1 - Terminal
Bonding Phone Number	Note: This field is only relevant to ISDN/PSTN participants. The phone number for Bonding dial-out calls. Bonding is a communication protocol that aggregates from two up to thirty 64 Kbps B channels together, to look like one large bandwidth channel.
Video Bit Rate	The video bit rate in units of kilobits per second. A value of 4294967295 denotes auto, and in this case, the rate is computed by the MCU.
IP Address	Note: This field is only relevant to IP participants. The IP address of the participant. An address of 4294967295 indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Signaling Port	Note: This field is only relevant to IP participants. The signaling port used for participant connection. A value of 65535 is ignored by MCU.
H.323 Participant Alias Type/SIP Participant Address Type	Note: This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: 7 - E164 8 - H.323 ID 13 - Email ID 14 - Participant number For SIP participants, the address type, as follows: 1 - SIP URI 2 - Tel URL
H.323 Participant Alias Name/SIP Participant Address	Note: This field is only relevant to IP participants. For H.323 participants: The participant alias. The alias may contain up to 512 characters. For SIP participants: The participant address. The address may contain up to 80 characters.

Event Fields for Event 1001 - NEW UNDEFINED PARTY CONTINUE 1

Field	Description
Encryption	Indicates the participant's encryption setting as follows: 0 - The participant is <i>not</i> encrypted. 1 - The participant is encrypted. 2 - Auto. The conference encryption setting is applied to the participant.
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.

Event Fields for Event 20 - BILLING CODE

Field	Description
Participant Name	The name of the participant who added the billing code.
Participant ID	The identification number, as assigned by the MCU, of the participant who added the billing code.
Billing Info	The numeric billing code that was added (32 characters).

Event Fields for Event 21 - SET PARTICIPANT DISPLAY NAME

Field	Description
Participant Name	The original name of the participant, for example, the name automatically assigned to an undefined participant, such as, " <conference name="">_(000)".</conference>
Participant ID	The identification number assigned to the participant by the MCU.
Display Name	The new name assigned to the participant by the user, or the name sent by the end point.

Event Fields for Event 22 - DTMF CODE FAILURE

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Incorrect Data	The incorrect DTMF code entered by the participant, or an empty field "" if the participant did not press any key.
Correct Data	The correct DTMF code, if known.

Field	Description
Failure Type	The type of DTMF failure, as follows:
	2 - The participant did not enter the correct conference password.
	6 - The participant did not enter the correct chairperson password.
	12 - The participant did not enter the correct Conference ID.

Event fields for Event 26 - RECORDING LINK

Field	Description
Participant Name	The name of the Recording Link participant.
Participant ID	The identification number assigned to the Recording Link participant by the MCU.
Recording Operation	The type of recording operation, as follows: 0 - Start recording 1 - Stop recording 2 - Pause recording 3 - Resume recording 4 - Recording ended 5 - Recording failed
Initiator	Not supported.
Recording Link Name	The name of the Recording Link.
Recording Link ID	The Recording Link ID.
Start Recording Policy	The start recording policy, as follows: 1 - Start recording automatically as soon as the first participant connects to the conference. 2 - Start recording when requested by the conference chairperson via DTMF codes or from the Collaboration Server Web Client, or when the operator starts recording from the Collaboration Server Web Client.

Event Fields for Event 28 - SIP PRIVATE EXTENSIONS

Field	Description
Participant Name	The name of the participant.
Participant ID	The participant's identification number as assigned by the system.
Called Participant ID	The called participant ID.
Asserted Identity	The identity of the user sending a SIP message as it was verified by authentication.
Charging Vector	A collection of charging information.

Field	Description
Preferred Identity	The identity the user sending the SIP message wishes to be used for the P-Asserted-Header field that the trusted element will insert.

Event Fields for Event 30 - GATEKEEPER INFORMATION

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Gatekeeper Caller ID	The caller ID in the gatekeeper records. This value makes it possible to match the CDR in the gatekeeper and in the MCU.

Event fields for Event 31 - PARTICIPANT CONNECTION RATE

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.
Participant Current Rate	The participant line rate in Kbps.

Event Fields for Event 32

Field	Description
IP V6	IPv6 address of the participant's endpoint.

Event fields for Event 33 - PARTY CHAIR UPDATE

Field	Description
Participant Name	The participant name.
Participant ID	The identification number assigned to the participant by the MCU.
Chairperson	Possible values: True - participant is a chairperson False - Participant is not a chairperson participant (is a standard participant)

Event fields for Event 34 - PARTICIPANT MAXIMUM USAGE INFORMATION

Field	Description
Participant Name	The name of the participant.
Participant ID	The identification number assigned to the participant by the MCU.
Maximum Bit Rate	The maximum bit rate used by the participant during the call.
Maximum Resolution	The maximum resolution used by the participant during the call. Note: The reported resolutions are: CIF, SD, HD720, and HD1080. Other resolutions are rounded up to the nearest resolution. For example, 2SIF is reported as SD resolution.
Maximum Frame Rate	The maximum frame rate used by the participant during the call.
Participant Address	Note: This field is only relevant to IP participants. For H.323 participants, the participant alias. The alias may contain up to 512 characters. For SIP participants, the participant address. The address may contain up to 80 characters.

Event Fields for Event 35 - SVC SIP PARTICIPANT CONNECTED

Field	Description
Participant Name	The name of the participant. An empty field "" denotes an unidentified participant or a participant whose name is unspecified
Participant ID	The identification number assigned to the participant by the MCU.
Participant Status	The participant status, as follows: 0 - Idle 1 - Connected 2 - Disconnected 3 - Waiting for dial-in 4 - Connecting 5 - Disconnecting 6 - Partially connected. Party has completed H.221 capability exchange 7 - Deleted by a user 8 - Secondary. The participant could not connect the video channels and is connected via audio only 10 - Connected with problem 11 - Redialing
Receive line rate	Negotiated reception line rate
Transmit line rate	Negotiated transmission line rate

Field	Description
Uplink Video Capabilities	a.Number of uplink streams b.Video stream (multiple streams) i.Resolution width ii.resolution height iii.max frame rate iv.max line rate
Audio Codec	SAC, Other
Secondary Cause	е

Event Fields for Event 100 - USER TERMINATE CONFERENCE

Field	Description
Terminated By	The login name of the user who terminated the conference.

Event Fields for Events 102,103, 104 - USER DELETE PARTICIPANT, USER DISCONNECT PARTICIPANT, USER RECONNECT PARTICIPANT

Field	Description
User Name	The login name of the user who reconnected the participant to the conference, or disconnected or deleted the participant from the conference.
Participant Name	The name of the participant reconnected to the conference, or disconnected or deleted from the conference.
Participant ID	The identification number assigned to the participant by the MCU.

Event Fields for Event 106 - USER SET END TIME

Field	Description
New End Time	The new conference end time set by the user, in GMT.
User Name	The login name of the user who changed the conference end time.

Event Fields for Events 107 and 109 - OPERATOR MOVE PARTY FROM CONFERENCE and OPERATOR ATTEND PARTY

Field	Description
Operator Name	The login name of the user who moved the participant.

Field	Description
Party Name	The name of the participant who was moved.
Party ID	The identification number of the participant who was moved, as assigned by the MCU.
Destination Conf The name of the conference to which the participant was moved. Name	
Destination Conf ID	The identification number of the conference to which the participant was moved.

Event Fields for Events 108, 112 - OPERATOR MOVE PARTY TO CONFERENCE, OPERATOR ATTEND PARTY TO CONFERENCE

Field	Description
Operator Name	The login name of the operator who moved the participant to the conference.
Source Conf Name	The name of the source conference.
Source Conf ID	The identification number of the source conference, as assigned by the MCU.
Party Name	The name of the participant who was moved.
Party ID	The identification number assigned to the participant by the MCU.
Connection Type	The connection type, as follows: 0 - Dial-out 5 - Dial-in
Bonding Mode	Note: This field is only relevant to ISDN/PSTN participants. Possible values are: 0 - Bonding is disabled 1 - Bonding is enabled 255 - Auto
Number Of Channels	Note: This field is only relevant to ISDN/PSTN participants. The number of channels, as follows: 255 - Auto Otherwise, in range of 1 - 30
Net Channel Width	The bandwidth of each channel. This value is always 0 , which represents a bandwidth of 1B , which is the only bandwidth that is currently supported.
Net Service Name	The name of the Network Service. An empty field "" indicates the default Network Service.
Restrict	Indicates whether or not the line is restricted, as follows: 27 - Restricted line 28 - Non restricted line 255 - Unknown or not relevant

Field	Description
Voice Mode	Indicates whether or not the participant is an Audio Only participant, as follows: 0 - The participant is <i>not</i> an Audio Only participant 1 - The participant is an Audio Only participant 255 - Unknown
Number Type	Note: This field is only relevant to dial-out, ISDN/PSTN participants. The type of telephone number, as follows: 0 - Unknown 1 - International 2 - National 3 - Network specific 4 - Subscriber 6 - Abbreviated 255 - Taken from Network Service, default
Net SubService Name	Note: This field is only relevant to dial-out, ISDN/PSTN participants. The network sub-service name. An empty field "" means that MCU selects the default sub-service.
Number of Party Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. The number of participant phone numbers. In a dial-in connection, the participant phone number is the CLI (Calling Line Identification) as identified by the MCU. In a dial-out connection, participant phone numbers are the phone numbers dialed by the MCU for each participant channel.
Number of MCU Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. The number of MCU phone numbers. In a dial-in connection, the MCU phone number is the number dialed by the participant to connect to the MCU. In a dial-out connection, the MCU phone number is the MCU (CLI) number as seen by the participant.
Party and MCU Phone Numbers	Note: This field is only relevant to ISDN/PSTN participants. The participant phone numbers are listed first, followed by the MCU phone numbers.
Ident. Method	Note: This field is only relevant to dial-in participants. The method by which the destination conference is identified, as follows: 0 - Password 1 - Called phone number, or IP address, or alias 2 - Calling phone number, or IP address, or alias
Meet Method	Note: This field is only relevant to dial-in participants. The meet-me per method, as follows: 1 - Meet-me per MCU-Conference 3 - Meet-me per participant 4 - Meet-me per channel

Field	Description
Net Interface Type	The type of network interface between the participant and the MCU, as follows: 0 - ISDN 2 - H.323 5 - SIP
H243 Password	The H.243 password, or an empty field "" if there is no password.
Chair	Not supported. Always contains the value 0 .
Video Protocol	The video protocol, as follows: 1 - H.261 2 - H.263 3 - H.264* 4 - H.264 255 - Auto
Audio Volume	The broadcasting volume assigned to the participant. The value is between 1 (lowest) and 10 (loudest).
Undefined Type	The participant type, as follows: 0 - Defined participant. (The value in the formatted text file is "default".) 2 - Undefined participant. (The value in the formatted text file is "Unreserved participant".)
Node Type	The node type, as follows: 0 - MCU 1 - Terminal
Bonding Phone Number	Note: This field is only relevant to ISDN/PSTN participants. The phone number for Bonding dial-out calls.
Video Rate	Note: This field is only relevant to IP participants. The video rate in units of kilobits per second. A value of 4294967295 denotes auto, and in this case, the rate is computed by the MCU.
IP Address	Note: This field is only relevant to IP participants. The IP address of the participant. An address of 4294967295 indicates that no IP address was specified for the participant, and the gatekeeper is used for routing. In all other cases the address overrides the gatekeeper.
Call Signaling Port	Note: This field is only relevant to IP participants. The signaling port used for participant connection. A value of 65535 is ignored by MCU.

Field	Description
H.323 Party Alias Type/SIP Party Address Type	Note: This field is only relevant to IP participants. For H.323 participants, the alias type, as follows: 7 - E164 8 - H.323 ID 11 - URL ID alias type 12 - Transport ID 13 - Email ID 14 - Participant number For SIP participants, the address type, as follows: 1 - SIP URI 2 - Tel URL
H.323 Party Alias/SIP Party Address	Note: This field is only relevant to IP participants. For H.323 participants, the participant alias. The alias may contain up to 512 characters. For SIP participants, the participant address. The address may contain up to 80 characters.

Event Fields for Event 111 - OPERATOR BACK TO CONFERENCE PARTY

Field	Description
Operator Name	The login name of the operator moving the participant back to the conference.
Party Name	The name of the participant being moved.
Party ID	The identification number, as assigned by the MCU, of the participant being moved.

Event Fields for Events 2011, 2012, and 2016

Field	Description
IP V6	IPv6 address of the participant's endpoint.

Event Fields for Event 3010 - PARTICIPANT INFORMATION

Field	Description
Info1	The participant information fields.
Info2	These fields enable users to enter general information about the participant, such as the
Info3	participant's e-mail address.
Info4	The maximum length of each field is 80 characters.
VIP	Not supported. Always contains the value 0 .

Disconnection Cause Values



For an explanation of the disconnection causes, see Appendix A: Appendix A - Disconnection Causes.

Disconnection Cause Values

Value	Call Disconnection Cause
0	Unknown
1	Participant hung up
2	Disconnected by User
5	Resources deficiency
6	Password failure
20	H323 call close. No port left for audio
21	H323 call close. No port left for video
22	H323 call close. No port left for FECC
23	H323 call close. No control port left
25	H323 call close. No port left for video content
51	A common key exchange algorithm could not be established between the MCU and the remote device
53	Remote device did not open the encryption signaling channel
59	The remote devices' selected encryption algorithm does not match the local selected encryption algorithm
141	Called party not registered
145	Caller not registered
152	H323 call close. ARQ timeout
153	H323 call close. DRQ timeout
154	H323 call close. Alt Gatekeeper failure
191	H323 call close. Remote busy
192	H323 call close. Normal
193	H323 call close. Remote reject
194	H323 call close. Remote unreachable
195	H323 call close. Unknown reason
198	H323 call close. Small bandwidth

Value	Call Disconnection Cause
199	H323 call close. Gatekeeper failure
200	H323 call close. Gatekeeper reject ARQ
201	H323 call close. No port left
202	H323 call close. Gatekeeper DRQ
203	H323 call close. No destination IP value
204	H323 call close. Remote has not sent capability
205	H323 call close. Audio channels not open
207	H323 call close. Bad remote cap
208	H323 call close. Capabilities not accepted by remote
209	H323 failure
210	H323 call close. Remote stop responding
213	H323 call close. Master slave problem
251	SIP timer popped out
252	SIP card rejected channels
253	SIP capabilities don't match
254	SIP remote closed call
255	SIP remote cancelled call
256	SIP bad status
257	SIP remote stopped responding
258	SIP remote unreachable
259	SIP transport error
260	SIP bad name
261	SIP trans error TCP invite
300	SIP redirection 300
301	SIP moved permanently
302	SIP moved temporarily
305	SIP redirection 305
380	SIP redirection 380
400	SIP client error 400
401	SIP unauthorized

Value	Call Disconnection Cause
402	SIP client error 402
403	SIP forbidden
404	SIP not found
405	SIP client error 405
406	SIP client error 406
407	SIP client error 407
408	SIP request timeout
409	SIP client error 409
410	SIP gone
411	SIP client error 411
413	SIP client error 413
414	SIP client error 414
415	SIP unsupported media type
420	SIP client error 420
480	SIP temporarily not available
481	SIP client error 481
482	SIP client error 482
483	SIP client error 483
484	SIP client error 484
485	SIP client error 485
486	SIP busy here
487	SIP request terminated
488	SIP client error 488
500	SIP server error 500
501	SIP server error 501
502	SIP server error 502
503	SIP server error 503
504	SIP server error 504
505	SIP server error 505
600	SIP busy everywhere

Value	Call Disconnection Cause
603	SIP global failure 603
604	SIP global failure 604
606	SIP global failure 606

MGC Manager Events that are not Supported by the Collaboration Server

The following MGC Manager events are not supported by the Collaboration Server:



For details of these events see the MGC Manager User's Guide Volume II, Appendix A.

- Event 8 REMOTE COM MODE
- Event 11 ATM CHANNEL CONNECTED
- Event 12 ATM CHANNEL DISCONNECTED
- Event 13 MPI CHANNEL CONNECTED
- Event 14 MPI CHANNEL DISCONNECTED
- Event 15 H323 CALL SETUP
- Event 16 H323 CLEAR INDICATION
- Event 24 SIP CALL SETUP
- Event 25 SIP CLEAR INDICATION
- Event 27 RECORDING SYSTEM LINK
- Event 110 OPERATOR ON HOLD PARTY
- Event 113 CONFERENCE REMARKS
- Event 2108 OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 1
- Event 3001 CONFERENCE START CONTINUE 2
- Event 3108 OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 2
- Event 4001 CONFERENCE START CONTINUE 3
- Event 4108 OPERATOR MOVE PARTY TO CONFERENCE CONTINUE 3

Appendix D - Ad Hoc Conferencing and External Database Authentication

The RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Ad Hoc conferencing feature enables participants to start ongoing conferences on-the-fly, without prior definition when dialing an Ad Hoc-enabled Entry Queue. The created conference parameters are taken from the Profile assigned to the Ad Hoc-enabled Entry Queue.



External Database Authentication is not supported in the RealPresence Collaboration Server 1800.

Ad Hoc conferencing is available in two the following modes:

- Ad Hoc Conferencing without Authentication
 Any participant can dial into an Entry Queue and initiate a new conference if the conference does not exist. This mode is usually used for the organization's internal Ad Hoc conferencing.
- Ad Hoc Conferencing with External Database Authentication
 In this mode, the participant's right to start a new conference is validated against a database.

The external database application can also be used to validate the participant's right to join an ongoing conference. Conference access authentication can be:

- Part of the Ad Hoc conferencing flow where the participants must be authorized before they can enter the conference created in the Ad Hoc flow.
- Independent of Ad Hoc conferencing where conference access is validated for all conferences running on the MCU regardless of the method in which the conference was started.

Ad Hoc Conferencing without Authentication

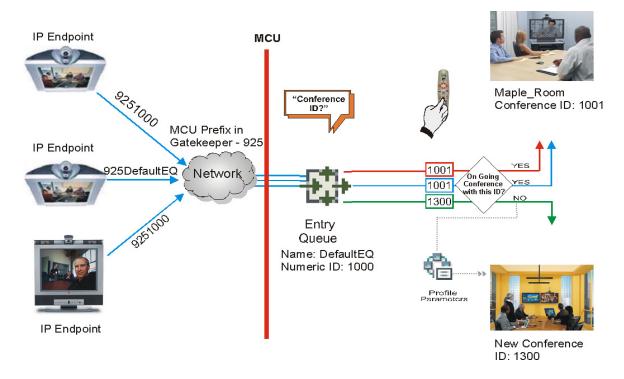
A participant dials in to an Ad Hoc-enabled Entry Queue and starts a new conference based on the Profile assigned to the Entry Queue. In this configuration, any participant connecting to the Entry Queue can start a new conference, and no security mechanism is applied. This mode is usually used in organizations where Ad Hoc conferences are started from within the network and without security breach.

A conference is started using one of the following method:

- 1 The participant dials in to the Ad Hoc-enabled Entry Queue.
- 2 The Conference ID is requested by the system.
- 3 The participant inputs a Conference ID via his/her endpoint remote control using DTMF codes.

4 The MCU checks whether a conference with the same Conference ID is running on the MCU. If there is such a conference, the participant is moved to that conference. If there is no ongoing conference with that Conference ID, the system creates a new conference, based on the Profile assigned to the Entry Queue, and connects this participant as the conference chairperson.

Ad Hoc Conference Initiation without Authentication



To enable this workflow, the following components must be defined in the system:

- An Entry Queue IVR Service with the appropriate audio file requesting the Conference ID
- An Ad Hoc-enabled Entry Queue with an assigned Profile

Ad Hoc Conferencing with Authentication

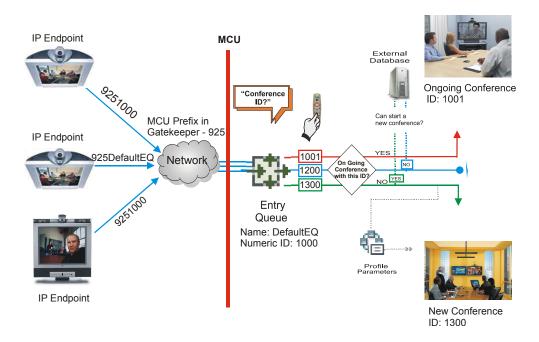
The MCU can work with an external database application to validate the participant's right to start a new conference. The external database contains a list of participants, with their assigned parameters. The conference ID entered by the participant is compared against the database. If the system finds a match, the participant is granted the permission to start a new conference.

To work with an external database application to validate the participant's right to start a new conference, the Entry Queue IVR Service must be configured to use the external database application for authentication. In the external database application, you must define all participants (users) with rights to start a new conference using Ad Hoc conferencing. For each user defined in the database, you enter the conference ID, Conference Password (optional) and Chairperson Password (when applicable), billing code, Conference general information (corresponding to the User Defined 1 field in the Profile properties) and user's PIN code. The same user definitions can be used for conference access authentication, that is, to determine who can join the conference as a participant and who as a chairperson.

Entry Queue Level - Conference Initiation Validation with an External Database Application

Starting a new conference with external database application validation entails the following steps:

Conference Initiation Validation with External Database Application



- 1 The participant dials in to an Ad Hoc-enabled Entry Queue.
- 2 The participant is requested to enter the Conference ID.
- 3 The participant enters the conference ID via his/her endpoint remote control using DTMF codes. If there is an ongoing conference with this Conference ID, the participant is moved to that conference where another authentication process can occur, depending on the IVR Service configuration.
- 4 If there is no ongoing conference with that Conference ID, the MCU verifies the Conference ID with the database application that compares it against its database. If the database application finds a match, the external database application sends a response back to the MCU, granting the participant the right to start a new ongoing conference.
 - If this Conference ID is not registered in the database, the conference cannot be started and this participant is disconnected from the Entry Queue.
- 5 The external database contains a list of participants (users), with their assigned parameters. Once a participant is identified in the database (according to the conference ID), his/her parameters (as defined in the database) can be sent to the MCU in the same response granting the participant the right to start a new ongoing conference. These parameters are:
 - Conference Name
 - Conference Billing code
 - Conference Password
 - Chairperson Password

- Conference Information, such as the contact person name. These fields correspond to Info 1, 2 and 3 fields in the Conference Properties Information dialog box.
- Maximum number of participants allowed for the conference
- > Conference Owner

These parameters can also be defined in the conference Profile. In such a case, parameters sent from the database overwrite the parameters defined in the Profile. If these parameters are not sent from the external database to the MCU, they will be taken from the Profile.

- 6 A new conference is started based on the Profile assigned to the Entry Queue.
- 7 The participant is moved to the conference. If no password request is configured in the Conference IVR Service assigned to the conference, the participant that initiated the conference is directly connected to the conference, as its chairperson.
 - If the Conference IVR Service assigned to the conference is configured to prompt for the conference password and chairperson password, without external database authentication, the participant has to enter these passwords in order to join the conference.

To enable this workflow, the following components must be defined in the system:

- A Conference IVR Service with the appropriate prompts. If conference access is also validated with the external database application it must be configured to access the external database for authentication.
- An Entry Queue IVR Service configured with the appropriate audio prompts requesting the Conference ID and configured to access the external database for authentication.
- Create a Profile with the appropriate conference parameters and the appropriate Conference IVR Service assigned to it.
- An Ad Hoc-enabled Entry Queue with the appropriate Entry Queue IVR Service and Conference Profile assigned to it.
- An external database application with a database containing Conference IDs associated with participants and their relevant properties.
- Define the flags required to access the external database in System Configuration.
 For more information, see MCU Configuration to Communicate with an External Database Application.

Conference Access with External Database Authentication

The MCU can work with an external database application to validate the participant's right to join an existing conference. The external database contains a list of participants, with their assigned parameters. The conference password or chairperson password entered by the participant is compared against the database. If the system finds a match, the participant is granted the permission to access the conference.

To work with an external database application to validate the participant's right to join the conference, the Conference IVR Service must be configured to use the external database application for authentication.

Conference access authentication can be performed as:

 Part of the Ad Hoc conferencing flow where the participants must be authorized before they can enter the conference created in the Ad Hoc flow

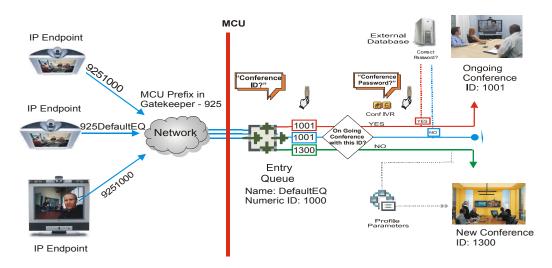
 Independent of Ad Hoc conferencing where conference access is validated for all conferences running on the MCU regardless of the method in which the conference was started.

Conference access authentication can be implemented for all participants joining the conference or for chairpersons only.

Conference Access Validation - All Participants (Always)

Once the conference is created either via an Ad Hoc Entry Queue, or a standard ongoing conference, the right to join the conference is authenticated with the external database application for all participants connecting to the conference.

Conference Access - Conference Password validation with External Database Application



Joining the conference entails the following steps:

- When the conference is started (either in the Ad Hoc flow or in the standard method), all participants
 connecting to the conference are moved to the Conference IVR queue where they are prompted for
 the conference password.
- When the participant enters the conference password or his/her personal password, it is sent to the external database application for validation.
- If there is a match, the participant is granted the right to join the conference. In addition, the external database application sends to the MCU the following parameters:
 - Participant name (display name)
 - Whether or not the participant is the conference chairperson
 - ➤ Participant Information, such as the participant E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the *Participant Properties Information* dialog box.

If there is no match (i.e. the conference or personal password are not defined in the database), the request to access the conference is rejected and the participant is disconnected from the MCU.

- If the Conference IVR Service is configured to prompt for the chairperson identifier and password, the participant is requested to enter the chairperson identifier.
 - > If no identifier is entered, the participant connects as a standard, undefined participant.

- If the chairperson identifier is entered, the participant is requested to enter the chairperson password.
 In this flow, the chairperson password is **not** validated with the external database application, only with the MCU.
 - > If the correct chairperson password is entered, the participant is connected to the conference as its chairperson.
 - > If the wrong password is entered, he/she is disconnected from the conference.

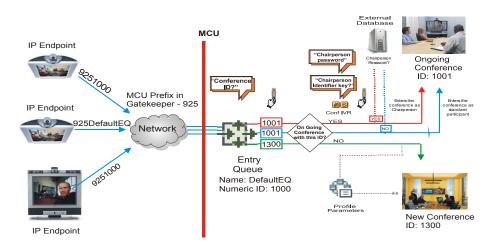
To enable conference access validation for all participants the following conferencing components are required:

- The external database must hold the conference password or the participant personal password/PIN code or the participant's Alias.
- The Conference IVR Service assigned to the conference (defined in the Profile) must be configured
 to authenticate the participant's right to access the conference with the external database application
 for all requests. In addition it must be configured to prompt for the Conference Password.

Conference Access Validation - Chairperson Only (Upon Request)

An alternative validation method at the conference level is checking only the chairperson password with the external database application. All other participants can be checked only with the MCU (if the Conference IVR Service is configured to prompt for the conference password) or not checked at all (if the Conference IVR Service is configured to prompt only for the chairperson password).

Conference Access - Chairperson Password validation with external database application



Joining the conference entails the following steps:

- When the conference is started (either in the Ad Hoc flow or in the standard method), all participants
 connecting to the conference are moved to the conference IVR queue where they are prompted for
 the conference password.
- If the Conference IVR Service is configured to prompt for the Conference password, the participant
 is requested to enter the conference password. In this flow, the conference password is **not** validated
 with the external database application, only with the MCU.
 - > If the wrong password is entered, he/she is disconnected from the conference.

- If the correct conference password is entered, the participant is prompted to enter the chairperson identifier key.
 - > If no identifier is entered, the participant is connected to the conference as a standard participant.
- If the chairperson identifier is entered, the participant is prompted to enter the chairperson password.
- When the participant enters the chairperson password or his/her personal password, it is sent to the
 external database application for validation.
 - If the password is incorrect the participant is disconnected from the MCU.
- If there is a match, the participant is granted the right to join the conference as chairperson. In addition, the external database application sends to the MCU the following parameters:
 - Participant name (display name)
 - Participant Information, such as the participant E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the *Participant Properties Information* dialog box.

To enable conference access validation for all participants the following conferencing components are required:

- The external database must hold the Chairperson Password or the participant's Alias.
- The Conference IVR Service assigned to the conference (defined in the Profile) must be configured
 to check the external database for the Chairperson password only when the participant enters the
 chairperson identifier key (either pound or star). In addition, it must be configured to prompt for the
 chairperson identifier key and password.

System Settings for Ad Hoc Conferencing and External Database Authentication

Ad Hoc Settings

Before a participant can initiate an Ad Hoc conference (with or without authentication), the following components must be defined:

- Profiles
 - Defines the conference parameters for the conferences that will be initiated from the Ad Hoc-enabled Entry Queue. For more details, see Conference Profiles on page 7.
- Entry Queue IVR Service with Conference ID Request Enabled
 - The Entry Queue Service is used to route participants to their destination conferences, or create a new conference with this ID. For details, see IVR Services.
 - In Ad Hoc conferencing, the Conference ID is used to check whether the destination conference is already running on the MCU and if not, to start a new conference using this ID.
- Ad Hoc enabled Entry Queue
 - Ad Hoc conferencing must be enabled in the Entry Queue and a Profile must be assigned to the Entry Queue. In addition, an Entry Queue IVR Service supporting conference ID request. For details, see Entry Queues on page 7..

Authentication Settings

MCU Configuration

Usage of an external database application for authentication (for starting new conferences or joining ongoing conferences) is configured for the MCU in the System Configuration. For details, see MCU Configuration to Communicate with an External Database Application .

• Entry Queue IVR Service with Conference Initiation Authentication Enabled

Set the Entry Queue IVR Service to send authentication requests to the external database application to verify the participant's right to start a new conference according to the Conference ID entered by the participant. For details, see Enabling External Database Validation for Starting New Ongoing Conferences.

• Conference IVR Service with Conference Access Authentication Enabled

Set the Conference IVR Service to send authentication requests to the external database application to verify the participant's right to connect to the conference as a standard participant or as a chairperson. For details, see Enabling External Database Validation for Conferences Access.

External Database Application Settings

The external database contains a list of participants (users), with their assigned parameters. These parameters are:

- Conference Name
- Conference Billing code
- Conference Password
- Chairperson Password
- ➤ Conference Information, such as the contact person name. These fields correspond to Info 1, 2 and 3 fields in the *Conference Properties Information* dialog box.
- Maximum number of participants allowed for the conference
- Conference Owner
- Participant name (display name)
- Participant Information, such as the participant E-mail. These fields correspond to Info 1, 2, 3 and 4 fields in the Participant Properties Information dialog box.

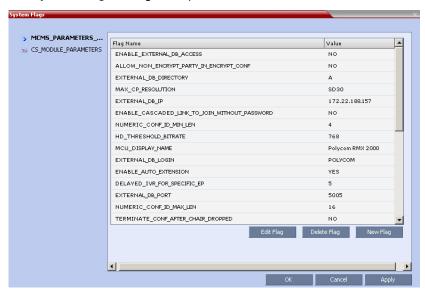
MCU Configuration to Communicate with an External Database Application

To enable the communication with the external database application, several flags must be set in the System Configuration.

To set the System Configuration flags:

1 On the Setup menu, click System Configuration.

The System Flags dialog box opens.



2 Modify the values of the following flags:

Flag Values for Accessing External Database Application

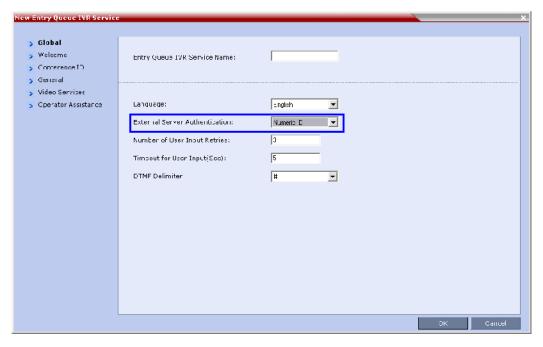
Flag	Description and Value
ENABLE_EXTERNAL_DB_ACCESS	The flag that enables the use of the external database application.
EXTERNAL_DB_IP	The IP address of the external database application server. default IP: 0.0.0.0.
EXTERNAL_DB_PORT	The port number used by the MCU to access the external application server. Default Port = 80.
EXTERNAL_DB_LOGIN	The user name defined in the external database application for the MCU.
EXTERNAL_DB_PASSWORD	The password associated with the user name defined for the MCU in the external database application.
EXTERNAL_DB_DIRECTORY	The URL of the external database application.

- 3 Click OK.
- 4 Reset the MCU for flag changes to take effect.

Enabling External Database Validation for Starting New Ongoing Conferences

The validation of the participant's right to start a new conference with an external database application is configured in the *Entry Queue IVR Service - Global* dialog box.

Set the External Server Authentication field to Numeric ID.



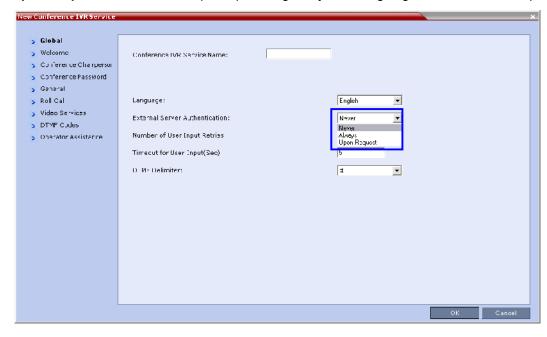
Enabling External Database Validation for Conferences Access

The validation of the participant's right to join an ongoing conference with an external database application is configured in the *Conference IVR Service - Global* dialog box.

You can set the system to validate all the participants joining the conference or just the chairperson.

- Set the External Server Authentication field to:
 - > Always to validate the participant's right to join an ongoing conference for all participants

• Upon Request - to validate the participant's right to join an ongoing conference as chairperson



Appendix E - Participant Properties Advanced Channel Information

The following appendix details the properties connected with information about audio and video parameters, as well as, problems with the network which can affect the audio and video quality.

Participant Properties - Channel Status Advanced Parameters

Field	Description
Media Info	
Algorithm	Indicates the audio or video algorithm and protocol.
Frame per packet (audio only)	The number of audio frames per packet that are transferred between the MCU and the endpoint. If the actual Frame per Packets are higher than Frame per Packets declared during the capabilities exchange, a Faulty flag is displayed.
Resolution (video only)	Indicates the video resolution in use. If the actual resolution is higher than resolution declared in the capabilities exchange, the Faulty flag is displayed. For example, if the declared resolution is CIF and the actual resolution is 4CIF, the Faulty flag is displayed.
Frame Rate (video only)	The number of video frames per second that are transferred between the MCU and the endpoint.
Annexes (video only)	Indicates the H.263 annexes in use at the time of the last RTCP report. If the actual annexes used are other than the declared annexes in the capabilities exchange, the Faulty flag is displayed.
Channel Index	For Polycom Internal use only.

Field	Description	
RTP Statistics		
Actual loss	The number of missing packets counted by the IP card as reported in the last RTP Statistics report. If a packet that was considered lost arrives later, it is deducted from the packet loss count. Packet loss is displayed with the following details:	
	 Accumulated N - number of lost packets accumulated since the channel opened. 	
	 Accumulated % - percentage of lost packets out of the total number of packets transmitted since the channel opened. 	
	 Interval N - number of packets lost in the last RTP report interval (default interval is 5 minutes). 	
	 Interval % - percentage of lost packets out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). 	
	 Peak - the highest number of lost packets in a report interval from the beginning of the channel's life span. 	
Out of Order	The number of packets arriving out of order. The	
	following details are displayed:	
	 Accumulated N - total number of packets that arrived out of order since the channel opened. 	
	 Accumulated % - percentage of packets that arrived out of order out of the total number of packets transmitted since the channel opened. Interval N - number of packets that arrived out of order in the last RTP report interval (default interval is 5 minutes). 	
	 Interval % - percentage of packets that arrived out of order out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). 	
	 Peak - the highest number of packets that arrived out of order in a report interval from the beginning of the channel's life span. 	

Field	Description	
Fragmented	Indicates the number of packets that arrived to the IP card fragmented (i.e., a single packet broken by the network into multiple packets). This value can indicate the delay and reordering of fragmented packets that require additional processing, but is not considered a fault.	
	 The Fragmented information is displayed with the following details Accumulated N - total number of packets that were fragmented since the channel opened. 	
	 Accumulated % - percentage of fragmented packets out of the total number of packets transmitted since the channel opened. 	
	 Interval N - number of fragmented packets received in the last RTP report interval (default interval is 5 minutes). 	
	 Interval % - percentage of fragmented packets out of the total number of packets transmitted in the last RTP report interval (default interval is 5 minutes). 	
	 Peak - the highest number of fragmented packets in a report interval from the beginning of the channel's life span. 	

Appendix F- Secure Communication Mode

The RealPresence Collaboration Server can be configured to work in *Secure Mode* or *Ultra Secure Mode*. For more information see Ultra Secure Mode and Flags Specific to Maximum Security Environments - Ultra Secure Mode.

In Secured mode the Collaboration Server and the Collaboration Server Web Client are configured to work with SSL/TLS.

In this mode, a SSL/TLS Certificate is installed on the MCU, setting the MCU Listening Port to secured port 443.

TLS is a cryptographic protocol used to ensure secure communications on public networks. TLS uses a Certificate purchased from a trusted third party Certificate Authority to authenticate public keys that are used in conjunction with private keys to ensure secure communications across the network.

The Collaboration Server supports:

- TLS 1.0
- SSL 3.0 (Secure Socket Layer)

SSL 3.0 utilizes 1024-bit RSA public key encryption.

TLS certificates can be generated using the following methods: CSR, PFX and PEM; each giving different options for *Encryption Key* length. The table below lists the *SIP TLS Encryption Key* length support for the various system components.

SIP TLS - Encryption Key Support by System Component

System Component	Key Generation Method	Key Length (bits)	Key generated by
SIP Signaling	CSR	2048	Collaboration Server
	PFX / PEM	1024 or 2048	User
Management	CSR	2048	Collaboration
LDAP	-		Server

Certificate Configuration and Management

All Polycom devices used in a Maximum Security Environment require security certificates.

For more details see the *Ultra Secure Mode* chapter, Certificate Management.

Certificate Template Requirements

The specific security certificate requirements for *Collaboration Servers* used in *Maximum Security Environments* are:

- Support of 2048-bit encryption keys.
- Support of Extended Key Usage (EKU) for both:
 - > Client Authentication
 - Server Authentication

The certificate template used by your *CA* server may need modification to meet the Collaboration Server requirements.

Certificate Requirements

Secure Mode

Table 5-126 on page **5-10** summarizes certificate requirements depending on the *Skip certificate validation* for user logging session field.

Ultra Secure Mode

In *Ultra Secure Mode*, each *Polycom* device must have security certificates for the entire *Chain Of Trust*.

The Collaboration Server must have:

• The public certificate of each server in the *CA Chain* or hierarchy that issued its certificate. For example: *RootCA* ↔ *IntermediateCA* ↔ *SubCA*

The public certificates of the chain that issued the administrator's identity certificate. For example: $UserRootCA \leftrightarrow UserIntermediateCA \leftrightarrow UserSubCA$

For more information see the Ultra Secure Mode chapter, Certificate Validation and Certificate Revocation .

Configure Certificate Management

Within a *PKI* environment, certificate revocation policies are used to ensure that certificates are valid. Certificates can expire or be revoked for various reasons (RFC 5280).

The Collaboration Server enforces these certificate revocation policies through *Certificate Revocation Lists* (*CRLs*). *CRLs* are required for each *CA Chain* in use by the Collaboration Server. These *CRL* files must be kept current. For more information see the *Ultra Secure Mode* chapter, Certificate Configuration and Management and (PKI) Public Key Infrastructure.

Switching to Secure Mode

The following operations are required to switch the Collaboration Server to Secure Mode:

- Purchase and Install the SSL/TLS certificate
- Modify the Management Network settings
- Create/Modify the relevant System Flags

Purchasing and Installing a Certificate

Once a certificate is purchased and received it is stored in the Collaboration Server and used for all subsequent secured connections. For more information see the *Ultra Secure Mode* chapter, Adding Certificates to the Certificate Repository .



Certificates are deleted when an administrator performs a *Restore Factory Defaults* with the *Comprehensive Restore* option selected.

Creating/Modifying System Flags

The following System Flags in system.cfg control secure communications.

- RMX_MANAGEMENT_SECURITY_PROTOCOL
- EXTERNAL_DB_PORT

Table 5-125, below, lists both flags and their settings.

If the System Flag, RMX_MANAGEMENT_SECURITY_PROTOCOL does not exist in the system, it must be created by using the Setup menu.

For more information see Modifying System Flags.

System Flags

Flag	Description
RMX_MANAGEMENT_S ECURITY_PROTOCOL	Enter the protocol to be used for secure communications. Default: TLSV1_SSLV3 (both)
EXTERNAL_DB_PORT	The external database server port used by the Collaboration Server to send and receive XML requests/responses. For secure communications set the value to 443. Default: 5005.

The Collaboration Server must be restarted for modified flag settings to take effect.

Enabling Secure Communication Mode

After the SSL/TLS Certificate is installed, secure communications are enabled by modifying the properties of the *Management Network* in the *Management Network* properties dialog box.

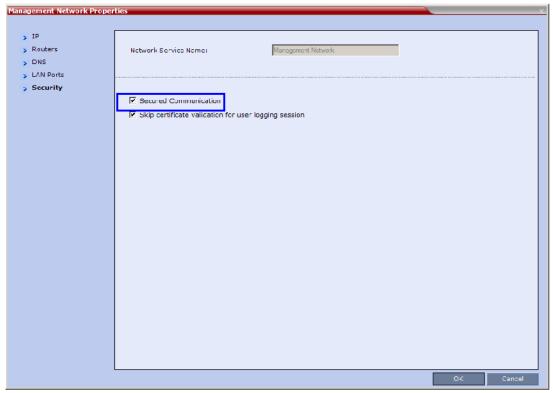
When Secure Communications Mode is enabled:

- Only https:// commands from the browser to the Control Unit IP Address of the Collaboration Server are accepted.
- The Collaboration Server listens only on secured port 443.
- All connection attempts on port 80 are rejected.
- A secure communication indicator () is displayed in the browser's status bar.

To enable secure communications mode:

- 1 In the Collaboration Server Management pane, click IP Network Services.
- 2 In the IP Network Services list pane, double-click the Management Network entry.
- 3 Click the Security tab.

The Management Security Properties dialog box is displayed.



- 4 Select the Secured Communication check box.
- 5 Select the Certificate Validation mode by checking or clearing the Skip certificate validation for user logging session field as set out in the following table:

Management Network Properties - Certificate Validation Mode

Field: Skip certificate validation for user logging session		
Status	RMX and Client Certificate Requirements	
Un-checked (Restricted Mode)	 The RMX must install a personal certificate issued by a CA. The Client must install a personal certificate issued by a CA. The public key of the CA must be installed in the RMX. Note: When the RMX Manager is the Client, all Personal Certificates in the workstation's Certification Repository are sent to the RMX. When using the RMX Web Client, Internet Explorer gives the user the option to select the Personal Certificate to be used from the workstation's Certification Repository. 	

Field: Skip certificate validation for user logging session		
Status RMX and Client Certificate Requirements		
Checked (Un-restricted Mode)	 The RMX must install a personal certificate issued by a CA. No additional configuration is required for the Client. 	

6 Click OK.

Alternate Management Network

The *Alternate Management Network* enables direct access to the Collaboration Server for support purposes. Access to the Alternate Management Network is via a cable connected to a workstation. The Alternate Management Network is accessible only via the dedicated LAN 3 port.

For more information see:

- Appendix G Configuring Direct Connections to the Collaboration Server
- Connecting to the Alternate Management Network .



Connection to the *Alternate Management Network* bypasses LAN and Firewall security. Strict control of access to *LAN 3* port is recommended.

Restoring Defaults

For details see Appendix J - Restoring Defaults .

Appendix G - Configuring Direct Connections to the Collaboration Server

Direct connection to the Collaboration Server is necessary if you want to:

- Modify the Collaboration Server's Factory Default Management Network settings without using the USB memory stick.
- Connect to the Collaboration Server's Alternate Management Network for support purposes.
- Connect to the Collaboration Server via a modem.



Direct connections to the Collaboration Server are not supported when the Collaboration Server is in *Ultra Secure Mode*. For more information see *Ultra Secure Mode*.

Management Network (Primary)

If you do not want to use the USB memory stick method of modifying the Collaboration Server's Management Network parameters, it is necessary to establish a direct connection between a workstation and the Collaboration Server.

Alternate Management Network

The Alternate Management Network enables direct access to the Collaboration Server for support purposes.

While being separate from all other networks, it has identical functionality to the *Management Network*.

Support personnel can log in and use it to manage the Collaboration Server if a connection to the *Management Network* cannot be made or if internet access to the host network is blocked by LAN security or a firewall.

The Alternate Management Network cannot be configured and operates according to factory defaults.

The administrator's **Login** name, **Password**, viewing and system permissions on the *Alternate Management Network* are the same as those on the *Management Network*.

Once logged in, the *RP Collaboration Server Web Client* behaves as if the administrator had logged in on the *Management Network*.



Connection to the *Alternate Management Network* bypasses LAN and Firewall security. Strict control of access to *LAN 3* port is recommended.



The Alternate Management Network is only available if Network Separation has not been performed. For more information, see Multiple Network Services.

Configuring the Workstation

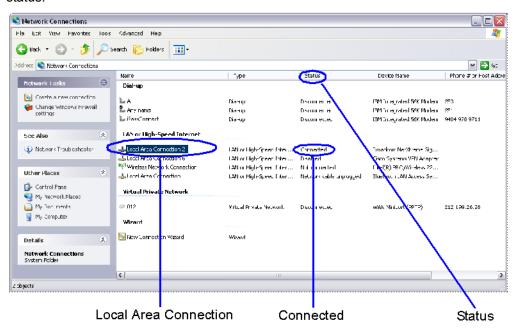
The following procedures show how to modify the workstation's networking parameters using the *Windows New Connection Wizard*.

For non-Windows operating systems an equivalent procedure must be performed by the system administrator.

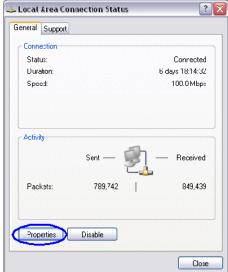
Before connecting directly, you must modify the *IP Address*, *Subnet Mask* and *Default Gateway* settings of the workstation to be compatible with either the Collaboration Server's *Default Management Network* or *Alternate Management Network*.

To modify the workstation's IP addresses:

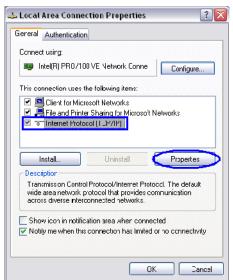
- 1 On the Windows Start menu, select Settings > Network Connections.
- 2 In the Network Connections window, double-click the Local Area Connection that has Connected status.



In the Local Area Connection Status dialog box, click the **Properties** button.

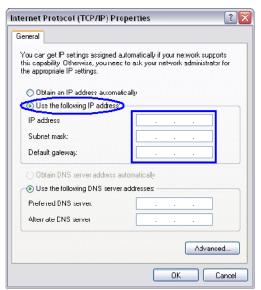


3 In the Local Area Connection Properties dialog box, select Internet Protocol [TCP/IP] > Properties.



4 In the Internet Protocol (TCP/IP) Properties dialog box, select **Use the following IP address**.

5 Enter the *IP address, Subnet mask* and *Default gateway* for the workstation.



The workstation's IP address should be in the same network neighborhood as the Collaboration Server's *Control Unit* IP address.

Example: IP address - near 192.168.1.nn



None of the reserved IP addresses listed in *Reserved IP Addresses* should be used for the IP Address.

The Subnet mask and Default gateway addresses should be the same as those for the Collaboration Server's Management Network.

The addresses needed for connection to either the Collaboration Server's *Default Management Network* or *Alternate Management Network* are listed in Table 5-127.

For more information about connecting to the *Alternate Management Network*, see Appendix G - Configuring Direct Connections to the Collaboration Server .

Reserved IP Addresses

	IP Address		
Network Entity	Management Network (Factory Default)	Alternate Network	
Control Unit IP Address	192.168.1.254	169.254.192.10	
Control Unit Subnet Mask	255.255.255.0	255.255.240.0	
Default Router IP Address	192.168.1.1	169.254.192.1	
Shelf Management IP Address	192.168.1.252	169.254.192.16	
Shelf Management Subnet Mask	255.255.255.0	255.255.240.0	

	IP Address	
Network Entity	Management Network (Factory Default)	Alternate Network
Shelf Management Default Gateway	192.168.1.1	169.254.192.1

6 Click the **OK** button.

Connecting to the Management Network

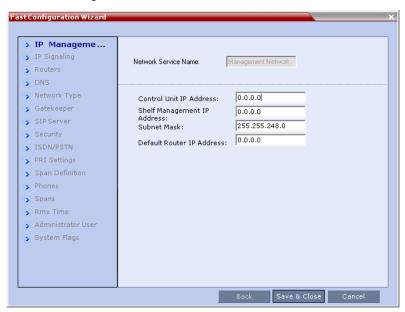
To connect directly to the Collaboration Server:

1 Using a LAN cable, connect the workstation to the LAN 2 Port on the Collaboration Server's back panel. Connect one LAN cable between the PC and LAN 1 on the Collaboration Server's back panel.



- 2 Connect the power cable and power the Collaboration Server On.
- 3 Start the *Collaboration Server Web Client* application on the workstation, by entering the factory setting *Management IP* address in the browser's address line and pressing **Enter**.
- 4 In the Collaboration Server Web Client Login screen, enter the default Username (POLYCOM) and Password (POLYCOM) and click the Login button.





If no *USB memory stick* is detected and **either**: this is the *First Time Power-up* **or** the *Default IP Service* has been deleted and the Collaboration Server has been reset, the following dialog box is displayed:

For more information about First-time Power-up and the *Fast Configuration Wizard* see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide*, Procedure 1: First-time Power-up.

- **5** Enter the following parameters using the information supplied by your network administrator:
 - Control Unit IP Address
 - Shelf Management IP Address
 - Control Unit Subnet Mask
 - Default Router IP Address
- 6 Click the Save & Close button.

The system prompts you to sign in with the new Control Unit IP Address.



- 7 Disconnect the LAN cable between the workstation and the LAN 2Port on the Collaboration Server's back panel.
- 8 Connect LAN 2Port on the Collaboration Server's back panel to the local network using a LAN cable.
- **9** Enter the new *Control Unit IP Address* in the browser's address line, using a workstation on the local network, and press **Enter** to start the *Collaboration Server Web Client* application.
- 10 In the Collaboration Server Web Client Login screen, enter the default Username (POLYCOM) and Password (POLYCOM) and click the Login button.

Connecting to the Alternate Management Network

Access to the *Alternate Management Network* is via a cable connected to a workstation. The *Alternate Management Network* is accessible only via the dedicated *LAN 3* port.



To connect to the Alternate Management Network:

- 1 Connect the cable between the Collaboration Server's LAN 3 port and the LAN port configured on the workstation.
- 2 Start the *Collaboration Server Web Client* application on the workstation, by entering http://169.254.192.10 (the *Control Unit IP Address*) in the browser's address line and pressing Enter.

The *Login* dialog box is displayed.



3 In the RealPresence Collaboration Server Welcome Screen, enter the administrator's Username and Password and click the Login button.

The RealPresence Collaboration Server Web Client starts and the Collaboration Server can be managed in the same manner as if you had logged on the Management Network.

Connecting to the Collaboration Server via Modem



This functionality is not supported by the Collaboration Server (RMX) 1800.

Remote access to the Collaboration Server's *Alternate Management Network* is supported via an external PSTN <=> IP modem.

To connect via modem to the Alternate Management Network the following procedures must be performed:

- 1 Procedure 1: Install the RMX Manager the web client enables direct access to the Collaboration Server for support purposes.
- **2 Procedure 2: Configure the modem** by assigning it an IP address on a specific subnet in the *Alternate Management Network*.
- 3 Procedure 3: Create a dial-up connection using the Windows New Connection Wizard.
- 4 Procedure 4: Connect to the Collaboration Server via the RMX Manager.

Procedure 1: Install the RMX Manager

Before installing the *RMX Manager*, verify that you have at least 150Mb of free space on your workstation. For more information see Installing the RMX Manager Application .

Procedure 2: Configure the Modem

Configure the modem as follows:

- IP address near 169.254.192.nn
- Subnet Mask 255.255.240.0



None of the reserved IP addresses listed in Table 5-127 on page **5-10** should be used for the IP Address

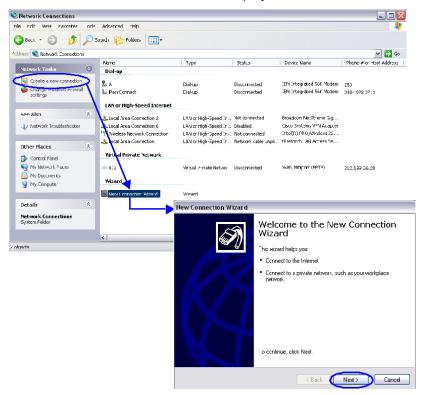
Procedure 3: Create a Dial-up Connection

To create a dial-up connection:

This procedure is performed once. Only the *Dial* field in the *Connect* applet (see step 10 on Click the Dial button to establish a connection to LAN 3 Port via the modem.) is modified for connection to different modems.

1 In Windows, navigate via the Control Panel to the Network Connections applet and select Create a new connection.

2 When the New Connection Wizard is displayed, click the Next button.



3 In the Network Connection Type box, select Connect to the Internet and click the Next button.



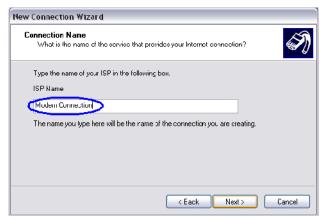
4 In the Getting Ready box, select Set up my connection manually and click the Next button.



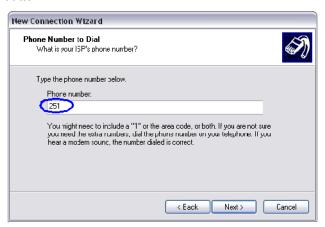
5 In the Internet Connection box, select Connect using dial-up modem and click the Next button.



6 In the Connection Name box, enter a Name for the modem connection (e.g. Modem Connection) and click the Next button.



7 In the *Phone Number to Dial* box, enter the **Phone Number** for the modem and click the **Next** button.



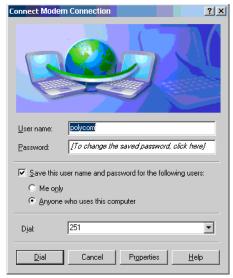
8 In the Connection Availability box, select Anyone's use and click the Next button.



9 In the *Internet Account Information* box, complete the *Username*, *Password* and *Confirm Password* fields and click the **Next** button.

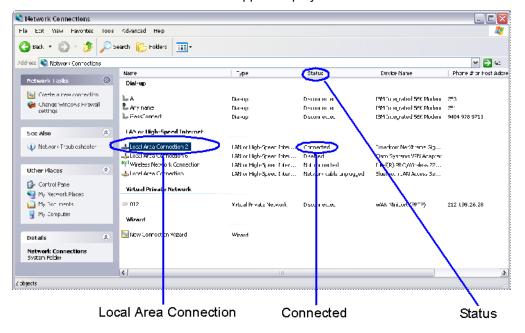


10 The *Connection* applet is displayed with the field values filled in as specified by the *New Connection Wizard*.



11 Click the **Dial** button to establish a connection to *LAN 3 Port* via the modem.

The Windows - Network Connections applet displays Connected status for the new connection.



Procedure 4: Connect to the Collaboration Server

To Connect using the RMX Manager:

To use the browser:

• In the browser's command line, enter http://<MCU Control Unit IP Address>/RmxManager.html and press Enter.

To use the Windows Start menu:

- 1 Click Start.
 - **a** If the RMX Manager is displayed in the recently used programs list, click RMX **Manager** in the list to start the application.

or

b Click All Programs.

The All Programs list is displayed.

c Select Polycom and then select RMX Manager.



The RMX Manager - Welcome screen is displayed.

Appendix H - Integration Into Microsoft Environments



Integration into Microsoft environment (using Lync endpoints) is supported in AVC CP Conferencing Mode only.

Overview

The Polycom® Visual Communications offers high quality video and audio multipoint conferencing by integrating the Polycom network devices and endpoints into Microsoft® platforms. The Polycom® RealPresence® Collaboration Server (Collaboration Server) system can be integrated into the following Microsoft environments:

- Office Communications Server 2007 environment (Microsoft R2, Wave 13)
- Lync Server 2010 environment (Microsoft Wave 14)



From Version 7.0.x, Microsoft R1 is not supported with Collaboration Server systems.

Point-to-point and multipoint audio and video meetings can be initiated from Office Communicator/ Lync client, Windows Messenger and Polycom video endpoints (HDX and VSX) when the environment components are installed and configured.

Multipoint calls are enabled when the Collaboration Server is installed in the Microsoft environment and is configured for unified communications. Routing to conferences can be performed by the Office Communications Server/Lync Server either by:

- Matched URI dialing using the SIP URI address.(both Office Communications Server and Lync Server)
- Numerical dialing enables a common dialing plan for Meeting Rooms across Office Communications Server and H.323 infrastructures (not available in Lync server environment).



Only TLS connections to the Collaboration Server will work, TCP connections will not work. The Collaboration Server does not support working with multiple Edge servers.

TLS certificates can be generated using the following methods: CSR, PFX and PEM; each giving different options for *Encryption Key* length. The table below lists the *SIP TLS Encryption Key* length support for the various system components.

SIP TLS - Encryption Key Support by System Component

System Component	Key Generation Method	Key Length (bits)	Key generated by
SIP Signaling	CSR	2048	Collaboration Server
	PFX / PEM	1024 or 2048	User
Management	CSR	2048	Collaboration Server
LDAP			

Conferencing Entities Presence

Conferencing entities (Meeting Rooms, Entry Queues and SIP Factories) can be registered with the SIP server (Office Communication Server or Lync server) enabling the addition of these conferencing entities to the buddy list while displaying their presence (availability status: Available, Offline, or Busy). Office Communication Server client or Lync Server client users can connect to conferencing entities directly from the buddy list.

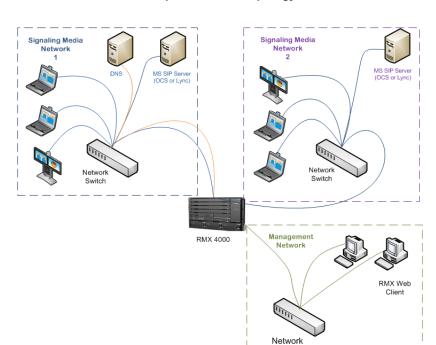
The configuration of the environment to enable Presence, is usually done once the basic configuration is completed.

For more details, see Adding Presence to Conferencing Entities in the Buddy List.

Multiple Networks

A more complex configuration, in which two Microsoft SIP servers are used (one Lync Server and one Office Communications Server) is also supported using the Collaboration Server Multiple Networks configuration.

In this configuration, each Microsoft SIP Server is defined in a Network Service of its own (in this case two IP Network Services are defined). A DNS server can be specified for each IP Network Service and for the RMX Management Network Service.



Collaboration Server Multiple Networks Topology

One *Network Service* including *ICE* can be configured per media card installed in the Collaboration Server as shown in the table below.

RMX - Media Cards vs Network Services including ICE

RMX	Total Media Cards	Network Services (Up to 2 per Media Card)	Network Services that Include ICE (1 per Media Card)
1500	1	2	1
2000	2	4	2
4000	4	8	4

Guidelines

- If ICE initialization fails in a Network Service:
 - ➤ The *Network Service* remains functional but without *ICE* capability.
 - > ICE capability on media cards that share the same Network Service also remain functional but without ICE capability.
 - > Other Network Services with ICE capability on other media cards are unaffected.
- A DNS server can be specified for each IP Network Service and for the Collaboration Server Management Network Service.

For more details about Multiple Networks configuration, see Multiple Network Services.

Interactive Connectivity Establishment (ICE)

Interactive Connectivity Establishment (ICE) provides a structure/protocol to unify the various NAT Traversal techniques that are used to cross firewalls.

It enables SIP based endpoints to connect while traversing a variety of firewalls that may exist between the calling endpoint (local) and the MCU or called endpoint (remote). It is the only way for remote Microsoft Office Communicator/Lync users to call into the enterprise without a VPN.

ICE Guidelines

- Collaboration Server ICE implementation complies with Microsoft ICE implementation.
- ICE is available only in IPv4 environment.
- ICE can be implemented in an environment that includes a STUN server and a Relay server (for example, Microsoft AV Edge server).
- The firewall must be UDP enabled.



When ICE over UDP is blocked in the firewall UDP port, the ICE connection through the TCP protocol is automatically used instead of UDP for fallback.

- The Collaboration Server must have a unique account in the Active Directory and must be registered with the Office Communications/Lync server.
- ICE is supported with Collaboration Server Multiple Networks.
- Ensure that the Collaboration Server system SIP signaling domain has been allowed on the Lync Server edge server to which you are federating (if your deployment does not include a DMA system).
- Content sharing (BFCP protocol) is not supported in ICE environment.

Connecting to the Collaboration Server in ICE Environment

The dialing methods that can be used by an endpoint to connect to another endpoint depends on the ICE environment: Local, Remote or Federation.

ICE Environmen



Local connection - a connection between the Collaboration Server and endpoints that reside within the same organization. For example, an endpoint in Zone A calls the Collaboration Server in Zone A.

Branch Office - a connection between an endpoint that is behind a firewall and the Collaboration Server that reside in the same zone. The user in the Branch Office can also place and receive calls from other enterprises and remote users. For example, Enterprise A also contains a branch office, which in this example is a Polycom HDX user who is behind more than one firewall.

Remote - a connection between Collaboration Server that resides within the organization and an endpoint that resides outside of the organization (on a WAN). For example, an endpoint on the internet that calls the Collaboration Server in Zone A. In such a case, the call has to traverse at least one firewall.

Federation - a connection between Collaboration Server that resides within one organization and an endpoint that resides within another organization. For example, an endpoint in Zone A calls the Collaboration Server in Zone B. The call has to traverse two or more firewalls.

Dialing Methods

The ICE protocol enables remote and federation connections using the registered user name for dialing. The endpoint connects to the Collaboration Server by entering the Collaboration Server registered user name in the following format:

[Collaboration Server registered user name]@[OCS/Lync server domain name]

For example:

rmx111@ilsnd.vsg.local

The call reaches the Transit Entry Queue of the Collaboration Server and via IVR is routed to the destination conference.

This method is added to the local connections and *Matched URI* and *Numerical Dialing* methods available in Microsoft Office Communication environment and the *Numerical Dialing* method available in the Lync server environment.

The following table summarizes the dialing methods and its availability in the various configurations.

Available dialing methods per Connection Type

	Matched URI Routing	Numerical Dialing	Registered User Name
Local	✓	✓	✓
Branch office	√ *	×	✓
Remote	√ *	×	✓
Federation	√ *	×	✓

^{*} To enable the *Matched URI dialing* in the federated environment to be able to connect to the Collaboration Server SIP signaling domain, you must also configure the Office Communications Server/Lync Server.

When federating an Office Communications Server/Lync Edge server with another Office Communications Server/Lync server environment, you need to include the FQDN of the Office Communications Server/Lync Edge server as well as the SIP signaling domain for federated environment. The SIP signaling domain is the FQDN of the Polycom DMA system or a Polycom Collaboration Server system (when your deployment does not include a DMA system).

For example, if company B wants to set up federation with company A and receive and send SIP calls that will be handled by the Polycom SIP signaling domain in company A, you need to add the FQDN of the company A Office Communications Server domain as well as the SIP signaling domain of company A to the list of internal SIP Server domains supported by the company B Office Communications Server/Lync Server environment.

Integrating the Collaboration Server into the Microsoft Office Communications Server Environment



From Version 7.0.x, Microsoft R1 is not supported with Collaboration Server systems.

When the Collaboration Server is integrated into the Office Communications Server environment, calls to conferences running on the Collaboration Server can be routed using Matched URI dialing and/or Numerical dialing.

Both routing methods (numerical dialing and Matched URI dialing) can be enabled simultaneously in the Office Communications Server and the Collaboration Server system or you can enable one of these methods, depending on your environment requirements.

In both methods, the Collaboration Server configuration is the same.

Setting the Matched URI Dialing Method

To enable the Matched URI dialing method the following tasks have to be completed:

Office Communications Server side:

- 1 Set the Static Route & Trusted Host for Collaboration Server in the Office Communications Server.
- 2 Optional if Load Balancer Server is present. Set the Static Route & Trusted Host for Collaboration Server in the Load Balancer server.

Collaboration Server side:

The following tasks are detailed in Configuring the Collaboration Server for Microsoft Integration.

- 1 Modify the Management Network Service to include the DNS server and set the Transport Type to TLS.
- 2 Create the security certificate (using one of the two available methods)
- 3 Define a SIP Network Service in the Collaboration Server and install the TLS certificate.
- 4 Modify and add the required system flags in the Collaboration Server System Configuration.
- **5 Optional.** Defining additional Entry Queues and Meeting Rooms in the Collaboration Server environment. For more information see *Defining a New Entry Queue* and *Creating a New Meeting Room.*

For a detailed description of the configuration of the Polycom conferencing components for the integration in Microsoft Office Communications Server 2007, see the *Polycom HDX and Collaboration Server Systems Integration with Microsoft Office Communications Server 2007 Deployment Guide.*

In ICE environment, to enable the Matched URI dialing in the federated environment to be able to connect to the Collaboration Server SIP signaling domain, you must also configure the Office Communications Server. When federating an Office Communications Server edge server with another Office Communications Server environment, you need to include the FQDN of the Office Communications Server edge server as well as the SIP signaling domain for federated environment. The SIP signaling domain is the FQDN of the Polycom DMA system or a Polycom Collaboration Server system (when your deployment does not include a DMA system).

Note: The RMX does not support working with multiple edge servers.

For example, if company B wants to set up federation with company A and receive and send SIP calls that will be handled by the Polycom SIP signaling domain in company A, you need to add the FQDN of the company A Office Communications Server domain as well as the SIP signaling domain of company A to the list of Internal SIP Server domains supported by the company B Office Communications Server environment.

Configuring the Office Communications Server for Collaboration Server Systems

To be able to work with the Office Communications Server, the Collaboration Server unit must be configured as a Trusted Host in the OCS. This is done by defining the IP address of the signaling host of each Collaboration Server unit as Trusted Host.

Meeting Rooms are usually not registered to the OCS, and Static Routes are used instead. Setting Static Routes in the OCS enables SIP entities / UAs to connect to conferences without explicit registration of conferences with the OCS.

Routing is performed by the OCS based on the comparison between the received URI and the provisioned static route pattern. If a match is found, the request is forwarded to the next hop according to the defined hop's address.

This is the recommended working method. It alleviates the need to create a user account in the OCS for each Meeting Room and Entry Queue. This also allows users to join ongoing conferences hosted on the MCU without registering all these conferences with OCS.

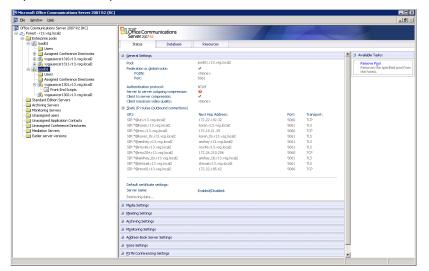
Entry Queues can also be for Ad-hoc conferencing enabling Office Communicator clients to dial to the Entry Queue and create a new ongoing conference using DTMF codes to enter the target conference ID. In such a case, other OC users will have to use that ID to join the newly created conference.

Setting the Trusted Host for Collaboration Server in the Office Communications Server

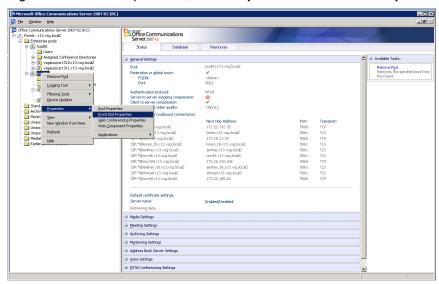
To set the Collaboration Server as trusted in OCS:

1 Open the OCS Management application.

2 Expand the Enterprise Pools list.

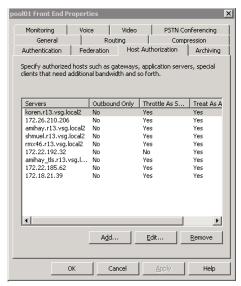


3 Right-click the server pool icon, click Properties > Front End Properties.

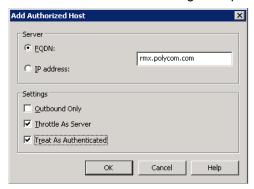


The Pool Front End Properties dialog box opens.

4 Click the Host Authorization tab.



5 Click the **Add** button to add the Collaboration Server as trusted host. The *Add Authorized Host* dialog box opens.



- 6 In the *Add Authorized Host* dialog box, enter the Collaboration Server *FQDN* name as defined in the DNS and will be used in the Static Routes definition.
- 7 In the Settings section, select the Throttle as Server and Treat As Authenticated check boxes.
- 8 Click OK.

The defined Collaboration Server is displayed in the trusted servers list in the server *Front End Properties—Host Authorization* dialog box.



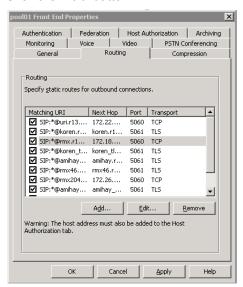
If routing between the Collaboration Server and the OCS using Static Routes is required, do not close this dialog box, and continue with the following procedure. If you do not want to define Static Routes, click OK to close this dialog box.

Setting the Static Route for Collaboration Server in the OCS

To add Collaboration Server to the Routing Roles:

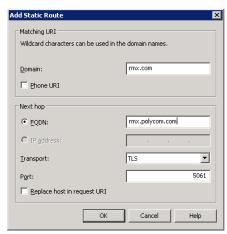
1 In the Front End Properties dialog box, click the Routing tab.

2 Click the Add button.



The Add Static Routes dialog box opens.

- 3 In the *Matching URI* section, enter the *Domain* name for the Collaboration Server. Any domain name can be used.
- **4** In the *Next hop* section enter the Collaboration Server *FQDN* name as defined in the DNS and is used in the *Host Authorization* definition.



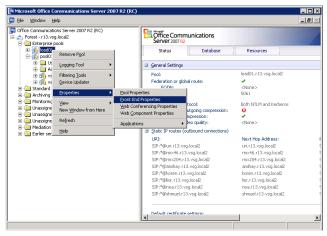
- 5 In the *Transport* field, select **TLS** to enable the dial-out from conferences to SIP endpoints.
- 6 Click OK. The new Route is added to the list of routes in the Front End Properties—Routes dialog box.
- 7 Click OK.

Setting the Static Route & Trusted Host for Collaboration Server in the Load Balancer Server (Optional)

If your network includes a Load Balancer server, the Collaboration Server unit must be configured as a trusted host in the Load Balancer server in the same way it is configured in the OCS. In addition, Static Routes must also be defined in the Load Balancer server in the same way it is configured in the OCS, however, the Load Balancer should be pointed to the OCS pool and not to the Collaboration Server directly. This configuration procedure is done in addition to the configuration in the OCS.

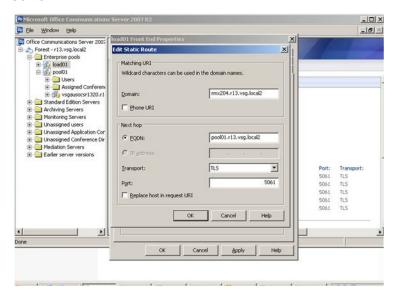
To set the Collaboration Server as trusted and define Static routes in the Load Balancer Server:

- 1 Open the OCS Management application.
- 2 Expand the Enterprise Pools list.
- 3 Right-click the Load icon, click Properties > Front End Properties.



The Load Front End Properties dialog box opens.

The definition procedure is the same as for setting the Collaboration Server as trusted and define Static routes in the OCS.



For details, see Setting the Trusted Host for Collaboration Server in the Office Communications Server.



Make sure that when defining the Static Route it is pointing to the OCS pool and not to the Collaboration Server directly.

Configuring the Collaboration Server System

The required tasks are detailed in Configuring the Collaboration Server for Microsoft Integration.

Dialing to an Entry Queue, Meeting Room or Conference Using the Matched URI Method

Once the Collaboration Server is configured for integration in the OCS environment (for details, see Configuring the Collaboration Server for Microsoft Integration), the preferred dialing mode to the conferencing entities such as Meeting Rooms, conferences and Entry Queues is direct dial in using the domain name defined in the OCS Static Routes. This eliminates the need to register the conferencing entities with the SIP server and to define a separate user for each conferencing entity in the Active Directory.

In such a case, after the first dial in, the conferencing entity will appear in the OC client directory for future use.

To dial in directly to a conference or Entry Queue:

Enter the conferencing entity SIP URI in the format: conferencing entity routing name@domain name

The domain name is identical to the domain name defined in the OCS Static Routes.

For example, if the domain name defined in the OCS static routes is lcs2007.polycom.com and the Routing Name of the Meeting Room is 4567, the participant enters 4567@lcs2007.polycom.com.

Another dialing method is to register the Entry Queues with the SIP Server and create a user for each Entry Queue in the Active Directory. In such a case, OC clients can select the Entry Queue from the Contacts list and dial to the Entry Queue.

Setting the Numerical Dialing Method

The Collaboration Server can be configured as a Voice Gateway in the OCS environment, enabling dialing in to meeting rooms using numbers instead of or in addition to SIP URI addresses which are long strings.

In such configuration, HDX or MOC users dial a number rather than a full SIP URI, simplifying the dialing, which is especially beneficial with the HDX remote control.

Such configuration also enables a common dialing plan for meeting rooms across OCS and H.323 infrastructures. In an integrated environment that also includes Microsoft Exchange Server and Polycom Conferencing Add-in for Microsoft Outlook, a single number can be inserted into a calendar invitation and it will be valid for OC client endpoints and H.323 endpoints.

This dialing method can be configured in parallel to the matching URI dialing method (using Static Routes).

Setting the Numerical Dialing for Collaboration Server Meeting Rooms

The following processes are required to set up the numerical dialing for the Collaboration Server Meeting Rooms in the OCS infrastructure:

OCS side:

- Configuring the Collaboration Server as a Routable Gateway The Collaboration Server (or DMA)
 must be set as a trusted voice gateway in the OCS infrastructure. This does not restrict Collaboration
 Server to just voice operation, rather it means that the Collaboration Server (or DMA) can be set as
 a destination for a voice route using the OCS management console.
 Setting the Collaboration Server as a trusted voice gateway also enables it to be used as a trusted
 gateway for static routes using URI matching.
- Establishing a Voice Route to the Collaboration Server "Voice" Gateway The Voice Route to the Collaboration Server (or DMA) must be configured in the OCS infrastructure.



If the Collaboration Server was previously defined as a Trusted Host for matching URI dialing method, this definition must be removed before configuring the Collaboration Server as a voice gateway. It will be defined as trusted host as part of the voice gateway configuration. For more details, see Optional. Removing the Collaboration Server from the Host Authorization List.

• Configure Office Communicator Users for Enterprise Voice.

Collaboration Server side:

The following tasks are detailed in Configuring the Collaboration Server for Microsoft Integration.

- 1 Modify the Management Network Service to include the DNS server and set the Transport Type to TLS.
- **2** Create the security certificate (using one of the two available methods)
- 3 Define a SIP Network Service in the Collaboration Server and install the TLS certificate.
- 4 Modify and add the required system flags in the Collaboration Server System Configuration.

5 Optional. Defining additional Entry Queues and Meeting Rooms in the Collaboration Server environment. For details see Meeting Rooms and Entry Queues.

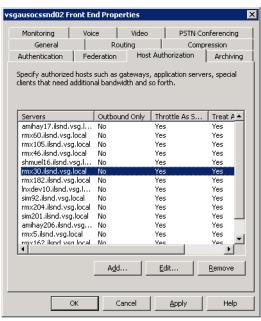
For a detailed description of the configuration of the Polycom conferencing components for the integration in Microsoft Office Communications Server 2007 see the *Polycom HDX and Collaboration Server Systems Integration with Microsoft Office Communications Server 2007 Deployment Guide.*

Optional. Removing the Collaboration Server from the Host Authorization List

If you have defined the Collaboration Server as Trusted Host to enable dialing using the Static Routes and you want to use numerical dialing in addition or instead of SIP URI dialing, you need to remove the current definition of the Collaboration Server and redefine it as a voice gateway.

To remove the definition of the Collaboration Server as trusted host from the Front End Properties:

- 1 In the OCS application, display the *Front End Properties* (right-click the Front End and select Properties).
- 2 Click the Host Authorization tab.
- 3 In the *Trusted Hosts* list, click the Collaboration Server entry and then click the **Remove** button.



4 Click OK.

Configuring the Collaboration Server as a Routable Gateway

The Collaboration Server must be set as a routable voice gateway in the Office Communications Server infrastructure. This does not restrict the Collaboration Server to just voice operation, rather it means that the Collaboration Server can be set as a destination for a voice route in the Office Communications Server infrastructure.

The Office Communications Server infrastructure uses the WMI class

MSFT_SIPTrustedAddInServiceSetting to store information for each voice gateway in the infrastructure. Typically, these gateways are Office Communications Server Mediation Servers, but in this case, the Collaboration Server is set as a voice gateway by creating a new instance of the class MSFT_SIPTrustedAddInServiceSetting.

Polycom recommends using the Office Communications Server 2007 R2 Resource Kit Tools to accomplish this.

To set up the Collaboration Server/DMA as a Voice Gateway:

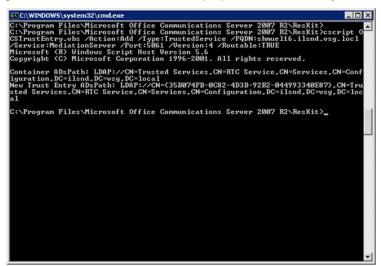
1 Download and install the Office Communications Server 2007 R2 Resource Kit Tools from the following URL:

http://www.microsoft.com/downloads/details.aspx?familyid=9E79A236-C0DF-4A72-ABA6-9A9602A93ED 0&displaylang=en

- 2 Open a command prompt and navigate to where you installed the resource kit. For example, C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\.
- **3** Run the following command:

cscript OCSTrustEntry.vbs /action:add /type:trustedservice /fqdn:<your FQDN> /service:MediationServer /port:5061 /version:4 /routable:TRUE

Where <\(your \) FQDN> is the FQDN of your Collaboration Server system. The script automatically generates the GUID discover the proper Active Directory container to store the object.



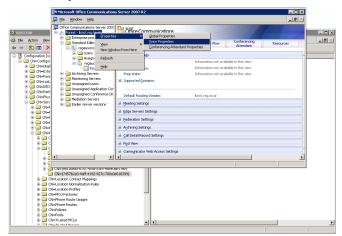
Your Collaboration Server system is now established as a trusted gateway by all Office Communications Server pools in the domain. It is displayed in the list of voice gateways when you establish a voice route.

Establishing a Voice Route to the Collaboration Server "Voice" Gateway

The OCS infrastructure enables you to establish a voice route to a voice gateway. Typically, this means that all SIP INVITEs to phone numbers which match a particular pattern will be routed to a specific gateway. In this example, all INVITEs to numbers which start with "11" will be routed to Collaboration Server11 (DNS name rmx11.r13.vsq.local2).

To establish the voice route:

Open the OCS R2 management Console and right click on Forest and then click Properties > Voice Properties.



The Office Communications Server Voice Properties dialog box opens.

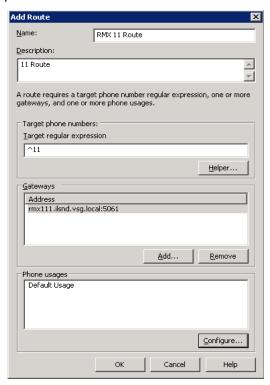
- 2 Click the Routes tab.
 - Office Communications Server Voice Properties Routes dialog box opens.
- 3 Click the Add button.



The Add Route dialog box opens.

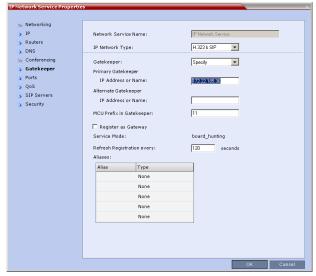
- 4 In the *Name* field, enter a name that will identify this voice route.
- **5** Optional. In the *Description* field, enter a description.

6 In the *Target Regular Expression* field enter **^** and the MCU prefix as defined in the gatekeeper. This prefix is also defined in the *Collaboration Server IP Network Service*.



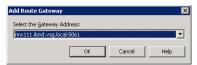
For example, if 11 is the Collaboration Server prefix defined in gatekeeper, enter **^11**. The circumflex expression "^11" causes this route to be applied to all numbers starting with "11".

If you have not defined such a prefix in the IP Network Service in the Collaboration Server configuration, you can add it later, using value entered here.



7 In the Gateways - Addresses box, click the Add button.

The Add Route Gateway dialog box opens.



- 8 Select the Collaboration Server gateway address that was set up in Configuring the Collaboration Server as a Routable Gateway that is displayed in the drop down list of gateways.
- 9 Click **OK** to save the address and return to the *Add Route* dialog box.
- **10** In the *Phone Usage* box, click the **Configure** button. The *Configure Phone Usage Records* dialog box opens.
- 11 In the *Available* box, click **Default Usage** and then click the > button.



The *Default Usage* option is displayed in the *Configured* box.

- 12 Click OK.
- 13 In the Add Route dialog box, click **OK** to save the new route.

Configuring Office Communicator Users for Enterprise Voice

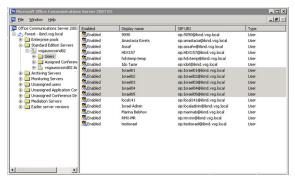
Each of the endpoints in the OCS environment must be set to use the voice route.

The setting is done in the Office Communications Server management console for all required users (endpoints) simultaneously or in the Active Directory for each of the Users (endpoints).

To Configure Office Communicator Users for Enterprise Voice in the Office Communications Server management console:

- Navigate to Start > All Programs > Administrative Tools > Office Communications Server 2007
 R2 to open the Office Communications Server management console.
- 2 Expand the Enterprise pool or Standard Edition server node where your users reside.
- 3 Expand the pool or server where your users reside, and then click the **Users** node.

4 In the right pane, right-click one or more users whom you want to configure, and then select **Configure users**.



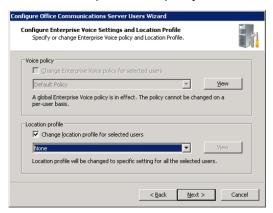
The Welcome to the Configure Users Wizard opens.

- 5 On the Welcome to the Configure Users Wizard dialog box, click Next.
- 6 On the Configure User Settings dialog box, click Next.
- 7 On the Configure Meeting Settings dialog box, click Next.
- 8 On the Configure User Settings specify meeting policy dialog box, click Next.
- 9 On the Configure Enterprise Voice dialog box, select Change Enterprise Voice Settings for selected users, and then click Enable Enterprise Voice.
- 10 Click Next.

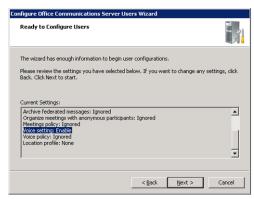


11 On the Configure Enterprise Voice Settings and Location Profile dialog box, select Change Enterprise Voice Policy for selected users.

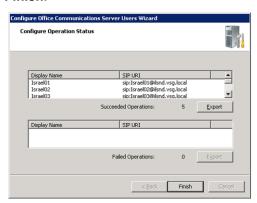
12 Select an Enterprise Voice policy from the list.



- 13 Select Change location profile for selected users.
- **14** Select a location profile from the list, and then click **Next**.
- 15 On the Ready to Configure Users dialog box, review the settings, and then click Next.



16 On the *Configure Operation Status* dialog box, verify that the operation succeeded, and then click **Finish**.



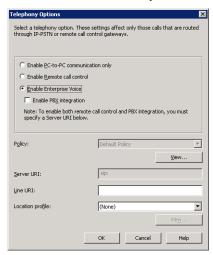
To Configure Office Communicator Users for Enterprise Voice in the in the Active Directory:

1 Open the Active Directory and navigate to the endpoint whose properties require changing.

- 2 Right-click the endpoint and select **Properties**. The *Properties* dialog box opens.
- 3 Click the Communications tab.



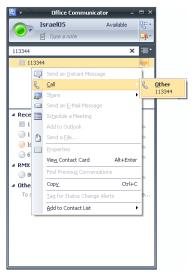
- 4 Click the **Telephony Settings Configure** button. The *Telephony Options* dialog box opens.
- 5 Select the **Enable Enterprise Voice** option.



- 6 Click **OK** to return to the *Properties Communications* dialog box.
- 7 Click OK.

Starting a Conferencing Call from the MOC

1 In the Office Communicator application, enter the number to dial, for example, 113344. This number is composed of the Collaboration Server Prefix in the Gatekeeper (for example, 11) and the Meeting Room ID, as defined on the Collaboration Server (for example, 3344).



- 2 Click Call, and then click Other. The call is routed to the Meeting Room on the Collaboration Server, and the caller that initiated the call connects as the conference chairperson.
- 3 The MOC User can then add video to the call, by selecting Add Video in the Office Communicator window.

Setting Simultaneous Numerical Dialing and Matched URI Routing

You can simultaneously set up an Collaboration Server for both numerical and Matched URI dialing. If you want to do this, follow these instructions:

- 1 Set the Collaboration Server as a trusted service (MediationServer) and a voice gateway using the instructions in Setting the Numerical Dialing Method.
- 2 Set up a matching URI route to the Collaboration Server/DMA by right-clicking the OCS Pool, selecting Properties > Front End Properties > Routing Tab and follow the instructions in Setting the Static Route for Collaboration Server in the OCS.



- When defining both routing methods, you cannot add an Collaboration Server as an Authorized Host using the Front End Properties > Host Authorization tab. There can only be one trusted service entry for the Collaboration Server even though there are two different routes to the Collaboration Server (i.e., Matched URI and numerical dialing). If the Matched URI routing method was previously defined and the Collaboration Server was set as trusted host, and you are adding the numerical dialing method, you have to remove the Collaboration Server from the Trusted Hosts list. For more details, see Optional. Removing the Collaboration Server from the Host Authorization List.
- Only TLS connections to the Collaboration Server will work, TCP connections will not work.

PFX Method - Creating the Security (TLS) Certificate in the OCS and Exporting the Certificate to the Collaboration Server Workstation

If you are using the PFX method to create and send the security certificate to the Collaboration Server, certificate files *rootCA.pem*, *pkey.pem* and *cert.pem* must be sent to the Collaboration Server unit. These files can be created and sent to the Collaboration Server in two methods:

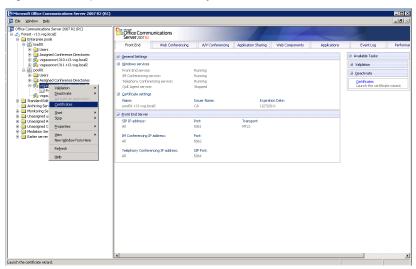
- The files rootCA.pem, pkey.pem and cert.pem are provided by a Certificate Authority and are sent
 independently or together with a password file to the Collaboration Server. This is the recommended
 method.
- Alternatively, the TLS certificate files are created internally in the OCS and exported to the Collaboration Server workstation from where the files can be downloaded to the Collaboration Server. If the certificate is created internally by the OCS, one *.pfx file is created. In addition, a text file containing the password that was used during the creation of the *.pfx file is manually created. Both files can then be sent from the Collaboration Server workstation to the Collaboration Server unit. When the files are sent to the Collaboration Server, the *.pfx file is converted into three certificate files: rootCA.pem, pkey.pem and cert.pem.

Sometimes, the system fails to read the *.pfx file and the conversion process fails. Resending *.pfx file again and then resetting the system may resolve the problem.

The following procedure describes how to create the *.PFX file in the OCS and export it so it can be sent to the Certificate Authority or to the Collaboration Server.

To create the TLS certificate in the Office Communications Server:

- 1 In the OCS Enterprise Pools tree, expand the Pools list and the server pool list.
- 2 Right-click the pool Front End entity, and click Certificate.



The Office Communicator Server Wizard Welcome window is displayed.

Click Next.

The Available Certificate Tasks window is displayed.

4 Select Create a New Certificate and click Next.



The Delayed or Immediate Request window is displayed.

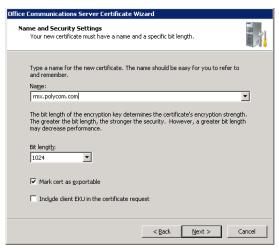
5 Select Send the Request immediately to an online certificate authority and click Next.



The Name and Security Settings window is displayed.

6 In the *Name* field, select the Collaboration Server name you entered in the *FQDN* field when defining the trusted host or as defined in the DNS server.

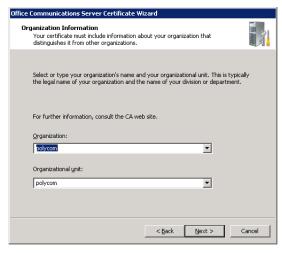
7 Select the Mark cert as exportable check box.



8 Click Next.

The Organization Information window is displayed.

9 Enter the name of the Organization and the Organization Unit and click Next.



Your Server's Subject Name window is displayed.

10 In the Subject name field, select the FQDN name of the Collaboration Server from the list or enter its name.

11 Keep the default selection in the Subject alternate name field and click Next.



- 12 If an error message is displayed, click Yes to continue.
 - The Geographical Information window is displayed.
- 13 Enter the geographical information as required and click Next.

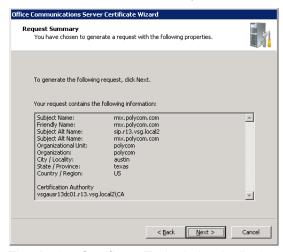


The Choose a Certification Authority window is displayed.

14 Ensure that the **Select a certificate authority from the list detected in your environment** option is selected and that the local OCS front end entity is selected.



- 15 Click Next.
 - The Request Summary window is displayed.
- 16 Click Next to confirm the listed parameters and create the requested certificate.



The Assign Certificate Task window is displayed.

17 Select Assign certificate later and click Next (MS R2).



The Certificate Wizard Completed window is displayed (MS R2).

18 Click Finish (MS R2).

Retrieving the Certificate from the OCS to be sent to the Collaboration Server Workstation

- 1 In the OCS Enterprise Pools tree, expand the Pools list and the Server Pool list.
- 2 Right-click the pool Front End entity, and select Certificate. The Available Certificate Tasks window is displayed.
- 3 Select Export a certificate to a *.pfx file and click Next.



The Available Certificates window is displayed.

4 Select the certificate Subject Name of the Collaboration Server and click Next.



The Export Certificate window is displayed.

5 Enter the path and file name of the certificate file to be exported or click the Browse button to select the path from the list.

The new file type must be *.pfx and its name must include the .pfx extension.



6 Select the Include all certificates in the certification path if possible check box and then click Next.

The Export Certificate Password window is displayed.

7 If required, enter any password. For example, *Polycom*.

8 Write down this password as you will have to manually create a password file in which this password will be displayed.

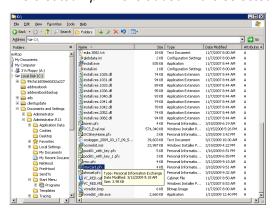


Click Next.

The Certificate Wizard Completed window is displayed.

9 Click Finish.

The created *.pfx file is added in the selected folder.



Optional. Creating the Certificate Password File (certPassword.txt)

If you have used a password when creating the certificate file (*.pfx), you must create a **certPassword.txt** file. This file will be sent to the Collaboration Server together with the *.pfx file.

To create the certPassword.txt file:

- 1 Using a text editor application, create a new file.
- **2** Type the password as you have entered when creating the certificate file. For example, enter *Polycom*.
- 3 Save the file naming it certPassword.txt (file name must be exactly as show, the Collaboration Server is case sensitive).

Supporting Remote and Federated Users in Office Communications Server ICE Environment

To enable the remote and Federation connections the following operations must be performed:

- Create an Active Directory account for the Collaboration Server that will be used for registering and operating in the MS ICE environment
- Enable the Collaboration Server User Account for Office Communication Server
- Configure the Collaboration Server for ICE dialing for more details, see Configuring the Collaboration Server for Federated (ICE) Dialing.



To place federated calls between Domain A and Domain B in ICE environment sub domains must be federated to the main domain or the Collaboration Server system must be installed on a main domain.

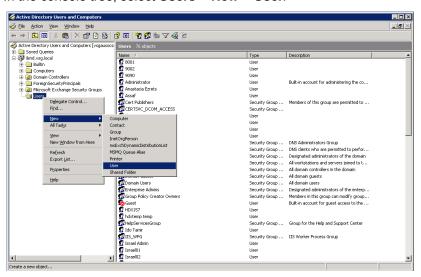
The Collaboration Server can also be set for Matched URI Routing and/or Numerical Dialing to Meeting Rooms. For more details, see Setting the Matched URI Dialing Method and Setting the Numerical Dialing Method.

Creating an Active Directory Account for the Collaboration Server

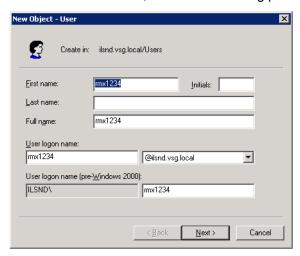
The User account created for the Collaboration Server is used for registration in the Office Communication Server and to automatically synchronize with the STUN and relay (Edge) servers.

To add the Collaboration Server user to the Active Directory:

- 1 Go to Start > Run and enter dsa.msc to open the Active Directory Users and Computers console
- 2 In the console tree, select Users > New > User.



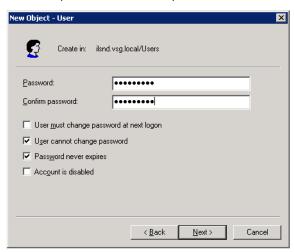
3 In the New User wizard, define the following parameters:



Active Directory - New User Parameters for the Collaboration Server

Field	Description	
First Name	Enter the name for the Collaboration Server user. This name will be used in the configuration of the ICE environment in the Collaboration Server.	
Full Name	Enter the same name as entered in the First Name field.	
User Login Name	Enter the same name as entered in the <i>First Name</i> field and select from the drop down list the domain name for this user. It is the domain name defined for the Office Communication Server.	

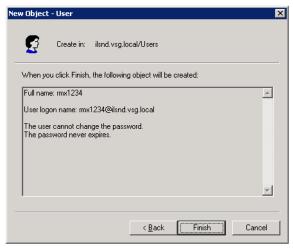
- 4 Click Next.
- **5** Enter the password that complies with the Active Directory conventions and confirm the password.



6 Select the options: **User cannot change password** and **Password never expires**. Clear the other options.

7 Click Next.

The system displays summary information.



8 Click Finish.

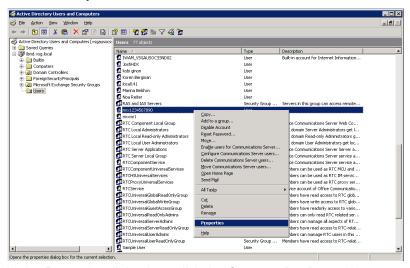
The new User is added to the Active Directory Users list.

Enabling the Collaboration Server User Account for Office Communication Server

The new Collaboration Server user must be enabled for registration with the Office Communications Server.

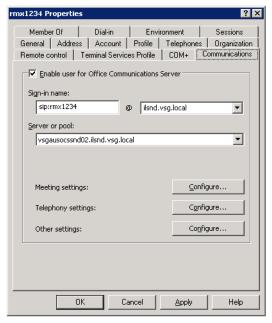
To enable the Collaboration Server User Account for Office Communication Server:

1 In the *Active Directory Users and Computers* window, right-click the Collaboration Server user and then click **Properties**.



2 In the *Properties* dialog box, click the **Communications** tab.

3 In the Sign in name field, enter the Collaboration Server user name in the format SIP:rmx user name (for example sip:rmx1234) and select the domain name (for example, ilsnd.vsg.local) as entered in the New User dialog box.



- 4 Select the Server or Pool from the list.
- 5 Click Apply and then OK.

Configure the Collaboration Server for ICE dialing

For details, see Configuring the Collaboration Server for Federated (ICE) Dialing.

Collaboration Server Integration into the Microsoft Lync Server 2010 and Lync Server 2013 Environments

From Version 7.8, the The RMX interoperability level with Lync 2013 is identical to Lync 2010. Lync 2013 is backward compatible with all RMX Lync 2010 features.

From Version 7.1, Collaboration Server systems can be integrated into the Microsoft Lync Server 2010 (Wave 14) environment.

In the Lync Server 2010 environment, only the Matched URI dialing (using the SIP URI address) is available as the call routing method.



Non-Lync endpoints connected to the same CP AVC-based conference as Lync endpoints running on the Collaboration Server, cannot participate in the desktop sharing session initiated by Lync participants.

Configuring the Polycom-Microsoft Solution

See the *Polycom HDX and Collaboration Server Systems Integration with Microsoft Office Communications Server 2007 Deployment Guide* for detailed steps on how to deploy a Polycom Collaboration Server system for use with the video conferencing solution in Microsoft Lync Server 2010 environment.

Call Admission Control (CAC)

Microsoft Call Admission Control (CAC), a protocol that enables bandwidth management via the Policy Server in federated (ICE) environment, is supported on the Collaboration Server.

The Policy server functionality enables the Lync server to manage the bandwidth allocated to the Lync client when connecting to another Lync client or a video conference running on the Collaboration Server. The bandwidth allocated by the Policy server may be the same or lower than the bandwidth requested by the Lync client, which is based on the line rate of the conference.

Guidelines

- Microsoft CAC is available only with:
 - A Lync server (Wave 14)
 - > Call Policy functionality enabled
 - > The Call Admission Control enabled for the Lync Clients
 - > ICE environment
 - Local network
- Microsoft CAC is applicable only to dial-in calls
- Additional configuration on the Microsoft side is not required. It is based on the existing ICE environment configuration.
- Additional configuration (setting a system flag) may be required on the Collaboration Server to modify
 the system behavior when CAC is enabled in a local network; closing the ICE channel or keeping it
 open.
- Setting an additional system flag may be required on the Collaboration Server when running Video Switching conferences.

For more details, see Collaboration Server Configuration for CAC Implementation.

FEC Support

Microsoft RTV FEC (Forward Error Correction) is supported in the Collaboration Server to control and correct packet loss when receiving and sending video streams using the Microsoft Lync Server 2010 communications software. All RTV resolutions and options, including B Frame, are supported.

Redundant video packets are sent over the network during video stream transmission. When packet loss occurs, FEC is automatically activated and the redundant packet is used to recover the lost packet.

When receiving video transmissions, packet loss automatically triggers FEC in the Collaboration Server. When sending video transmissions, Collaboration Server sends FEC packets when the RTCP RX report contains packet loss that is greater than or equal to 1 percent.

Media Over TCP

In previous Collaboration Server versions, media such as video, audio, content and FECC is transmitted using the UDP transport protocol. In version 7.7, mediaMedia is automatically transmitted through TCP when UDP, the default transport protocol, is not available. Media over TCP is supported using the Microsoft ICE environment.

The media transport protocol type (UDP/TCP) is displayed in the *Participant Properties - Channel Status - Advanced* dialog box.

The media transport protocol type is displayed for the following IP addresses:

- Collaboration Server IP Address
- Participant IP Address
- ICE Collaboration Server IP Address only when ICE is functional
- ICE Participant IP Address only when ICE is functional

Network Error Recovery

When a short network error occurs, for example 5 seconds, Collaboration Server automatically recovers, enabling calls in Microsoft Lync to continue the video or audio conference without disconnecting. However, when a longer network error occurs, the call is disconnected. The presence status mode is correctly updated from *Busy* to *Available*. There is no configuration required for this procedure.

SIP Dialog Recovery

Collaboration Server has the ability to automatically recover from a SIP dialog failure, which can occur in long duration calls in Meeting Rooms using the Microsoft Lync client. There is no configuration required for this procedure.

Content Sharing via Polycom CSS (Content Sharing Suite) Plug-in for Lync Clients

The Polycom CSS (Content Sharing Suite) Plug-in for Lync clients allows Lync clients to receive and send Content on a separate channel, without having to use the video channel. Content is transmitted using SIP BFCP. For more details, see Sharing Content via the Polycom CSS Plug-in for Lync Clients.

Configuring the Collaboration Server for Microsoft Integration

The Collaboration Server is integrated in Microsoft Office Communications Server R2 (Wave 13) and Microsoft Lync Server environments by setting its *Transport Type* (in the SIP server configuration) to **TLS** and creating a certificate that is sent to the Collaboration Server. This procedure is also required when encryption of SIP signaling is used.



From Version 7.0.x, Microsoft R1 is not supported with Collaboration Server systems.

In addition, if the DNS server was not enabled in the *Network Management Service* on the Collaboration Server, it must be enabled for the integration in Microsoft Office Communications Server (R2, Wave 13) and the Lync Server (Wave 14) environments.

Modify the Collaboration Server Management Network Service to Include the DNS Server

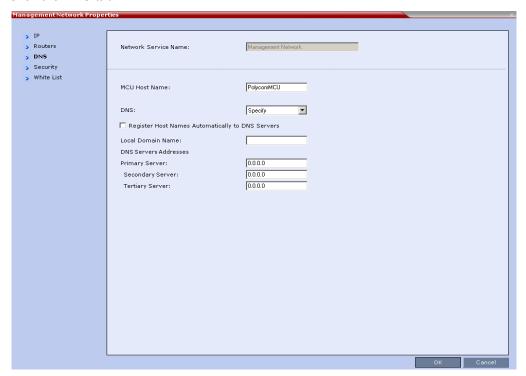
The *Management Network* that is defined during first entry setup does not include the definition of the DNS which is mandatory in Microsoft environment and has to be modified.



In *Multiple Networks* configurations, a *DNS* server can be specified for each *IP Network Service* and for the *Collaboration Server Management Network Service*.

To add the definition of the DNS to the Management Network in the Collaboration Server:

- 1 Using the Web browser, connect to the Collaboration Server.
- 2 In the Collaboration Server Management pane, expand the Rarely Used list and click IP Network Services.
- 3 In the *IP Network Services* pane, double-click **Management Service.**The *Management Network Properties IP* dialog box opens.
- 4 Click the DNS tab.



- 5 In the *DNS* field, select **Specify** to define the DNS parameters.
- **6** View or modify the following fields:

Management Network Properties - DNS Parameters

Field	Description	
MCU Host Name	Enter the name of the MCU on the network. This name must be identical to the FQDN name defined for the Collaboration Server in the OCS and DNS. Default name is Collaboration Server.	
Shelf Management Host Name	Displays the name of the entity that manages the Collaboration Server hardware. The name is derived from the MCU host name. Default is RMX_SHM.	
DNS	 Select: Off – if DNS servers are not used in the network. Specify – to enter the IP addresses of the DNS servers. Note: The IP address fields are enabled only if Specify is selected. 	
Register Host Names Automatically to DNS Servers	Select this option to automatically register the MCU Signaling Host and Shelf Management with the DNS server.	
Local Domain Name	Enter the name of the domain where the MCU is installed as defined in the Office Communications Server/Lync Server.	
DNS Servers Addresses:		
Primary Server	The static IP addresses of the DNS servers (the same servers defined in the Office Communications Server/Lync Server). A maximum of three servers can be defined.	
Secondary Server		
Tertiary Server	_	

7 Click OK.

Defining a SIP Network Service in the Collaboration Server and Installing the Security Certificate

Your RealPresence Collaboration Server system should be installed according to standard installation procedures. For details, see the *Polycom RealPresence Collaboration Server (RMX)* 1500/1800/2000/4000 *Getting Started Guide*.

When configuring the *Default IP Network Service* on first entry, or when modifying the properties of the existing *Default IP Network Service*, the SIP environment parameters must be set as described in this section.

The Security Certificate

There are two methods to create and send the security certificate that is required for configuration of the integration of the Collaboration Server in the Microsoft environment:

- The CSR method (recommended method for Microsoft Office Communications Server, Wave 13)
- The PFX method (Recommended method for Lync Server, Wave 14)

The CSR Method

In the CSR method, the security certificate is created as part of the *SIP Server* configuration in the IP Network Service configuration.

Using the CSR Method, the following processes are performed:

- Creating the certificate request (in the Default IP Network Service SIP Server dialog box).
- Sending the certificate request to a Certificate Authority.
- Receiving the certificate from the Certificate Authority.
- Installing the certificate in the Collaboration Server (in the Default IP Network Service SIP Server dialog box).

The PFX Method

In the PFX method, the security certificate is created in advance, in the Office Communications Server or Lync Server environment.

For detailed description of this procedure in the Office Communications Server environment, see PFX Method - Creating the Security (TLS) Certificate in the OCS and Exporting the Certificate to the Collaboration Server Workstation.

For detailed description of this procedure in the Lync Server environment, see the see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*

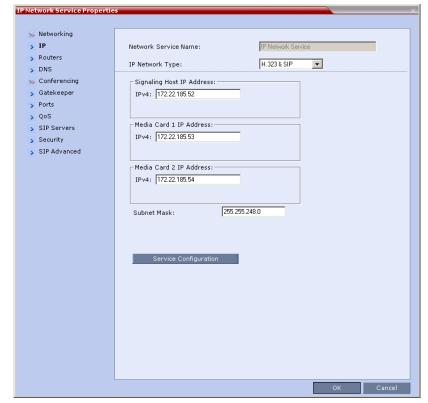


Certificates are deleted when an administrator performs a *Restore Factory Defaults* with the *Comprehensive Restore* option selected.

Configuring the Collaboration Server IP Network Service

To configure the Collaboration Server IP Network Service:

- 1 Using the Web browser, connect to the Collaboration Server.
- 2 In the RMX Management pane, expand the Rarely Used list and click IP Network Services.
- 3 In the IP Network Services pane, double-click the **Default IP Service** entry.



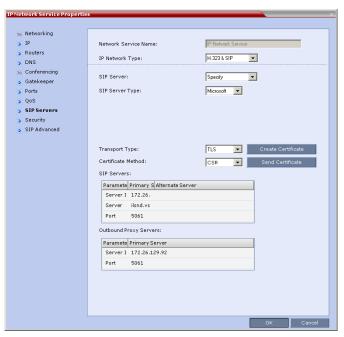
The *Default IP Service - Networking IP* dialog box opens.

- **4** Make sure the *IP Network Type* is set to **H.323 & SIP** even though SIP will be the only call setup used with Office Communications Server 2007.
- Make sure that the correct parameters are defined for the Signaling Host IP Address, Media Card 1 IP Address, Media Card 2 IP Address (RealPresence Collaboration Server (RMX) 2000/4000 if necessary), Media Card 3 IP Address (RealPresence Collaboration Server (RMX) 4000 if necessary), Media Card 4 IP Address (RealPresence Collaboration Server (RMX) 4000 if necessary) and Subnet Mask.



Make sure that the IP address of the Collaboration Server Signaling Host is the same one defined as a trusted host in Office Communications Server 2007/Lync Server 2010.

6 Click the SIP Servers tab.



- 7 In the SIP Server, select Specify.
- 8 In the SIP Server Type, select Microsoft.
- **9** Enter the IP address of the Office Communications Server 2007 or Lync Server 2010 and the *Server Domain Name* as defined in the OCS/Lync Server and in the *Management Network* for the DNS.
- 10 If not selected by default, change the Transport Type to TLS. The Create Certificate and Send Certificate buttons are enabled.
- 11 If you are using the CSR method, and the CSR option is not selected by default, change the Certificate Method to CSR.

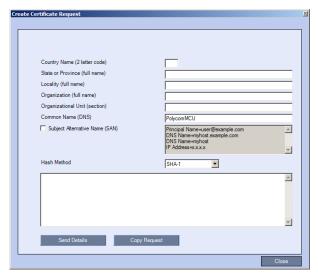
If you are using the PFX method, in the *Certificate Method* field select **PEM/PFX**. At this point the procedure changes according to the selected certificate method.

If you have selected PEM/PFX, skip to step Click the Send Certificate button. on Click the Send Certificate button.

CSR Method - Creating the Certificate

1 Click the Create Certificate button.

The Create Certificate Request dialog box is displayed.



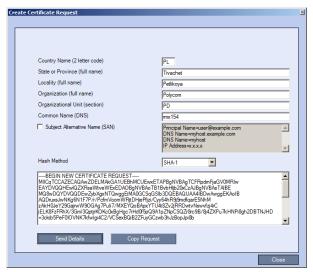
2 Enter information in all the following fields:

Create Certificate Request

Field	Description
Country Name	Enter any 2 letter code for the country name.
State or Province	Enter the full name of the state or province.
Locality	Enter the full name of the town/city/location.
Organization	Enter the full name of your organization for which the certificate will be issued.
Organizational Unit	Enter the full name of the unit (group or division) for which the certificate will be issued.
Common Name (DNS/IP)	Enter the DNS MCU Host Name. This MCU Host Name must also be configured in the Management Network Properties dialog box.
Subject Alternative Name	Ultra Secure Mode: Leave this unchecked.
Hash Method	Select the hash method to be used to hash the certificate request.

3 Click Send Details.

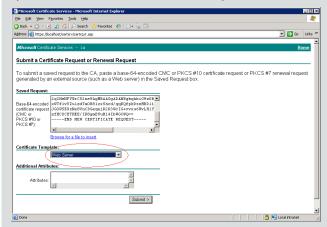
The Collaboration Server creates a *New Certificate Request* and returns it to the *Create Certificate Request* dialog box along with the information the user submitted.



- 4 Click Copy Request to copy the New Certificate Request to the workstation's clipboard.
- 5 Connect to your preferred Certificate Authority's website using the web browser.
- 6 Follow the purchasing instructions at the Certificate Authority's website.
- 7 Paste (Ctrl + V) the New Certificate Request as required by the Certificate Authority.



When creating the certificate request in the Certificate Authority site, make sure that the **Web Server** option is selected as the Certificate Template, as shown in the example below.



The Certificate Authority issues the TLS/SSL certificate, and sends the certificate to you by e-mail.



If the process of purchasing the certificate is short, you may leave the *IP Network Service - SIP Servers* dialog box open. Otherwise, close it without saving the changes to the Transport Type and Certificate Method.

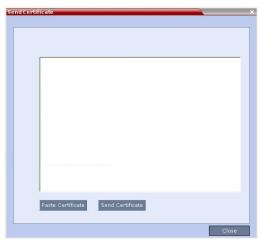
CSR Method - Sending the certificate

After you have received the certificate from the Certificate Authority:



If you have closed the *IP Network Service - SIP Servers* dialog box, repeat steps 1 to If you are using the CSR method, and the CSR option is not selected by default, change the Certificate Method to CSR. in the procedure Defining a SIP Network Service in the Collaboration Server and Installing the Security Certificate.

- 1 Open the Certificate Authority e-mail and Copy (Ctrl + C) the certificate information from the Certificate Authority's e-mail to the clipboard.
- 2 In the *IP Network Service SIP Servers* dialog box, click the **Send Certificate** button. The *Send Certificate* dialog box opens.
- 3 Click Paste Certificate to paste the clipboard content into the Send Certificate dialog box.



4 Click the Send Certificate button to send the certificate to the Collaboration Server.



- 5 Click the Close button.
- 6 In the IP Network Service SIP Servers dialog box, complete the SIP Servers definitions.

7 Click OK.

The MCU validates the certificate.

- If the certificate is not valid, an error message is displayed.
- If the certificate matches the private key, and the task is completed, a confirmation message indicating that the certificate was created successfully is displayed.



Once the certificate is installed in the Collaboration Server you can complete the definition procedure or continue with the Collaboration Server configuration for ICE dialing. For details, see Configuring the Collaboration Server for Federated (ICE) Dialing.

8 If no additional configuration is required, reset the Collaboration Server.

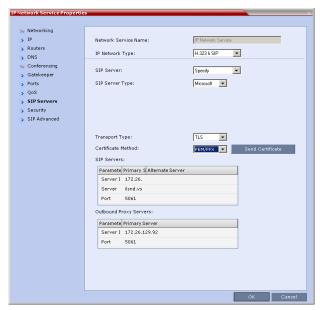


Reset can be performed after setting the system flags (for example, setting the MS_ENVIRONMENT flag). After system reset the Collaboration Server can register to the OCS server and make SIP calls.

PFX Method - Sending the Certificate

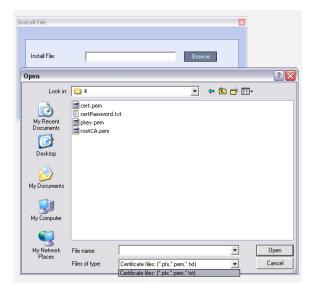
The PFX certificate request is created in the Microsoft Office Communications Server or Lync server. This certificate is received from the Certificate Authority it can be sent to the Collaboration Server, as described in the following procedure:

1 Click the Send Certificate button.



The Install File dialog box opens.

2 Click the Browse button.



The Open dialog box is displayed, letting you select the certificate file(s) to send to the MCU.

Depending on the method used when the certificate file(s) were created, send the certificate file(s) to the Collaboration Server according to the contents of the file set that was created:

- ➤ The certificate files *pkey.pem*, *cert.pem* and a *certPassword.txt*. The files were created by a Certificate Authority and are sent as is to the Collaboration Server together with the required password contained in the *certPassword.txt* file.

 This is the recommended method.
- > The files *pkey.pem* and *cert.pem*. The certificate files were created by a Certificate Authority and are sent as is to the Collaboration Server.
- ➤ A *.pfx file and a certPassword.txt file. The file certPassword.txt is manually created if the *.pfx file was created by the OCS using a password. The *.pfx file will be converted internally by the Collaboration Server using the password included in the certPassword.txt into three certificate files named pkey.pem and cert.pem.
- A *.pfx file if the certificate file was created in the OCS without using a password. The *.pfx file will be converted internally by the Collaboration Server into three certificate files named pkey.pem and cert.pem.
- 3 In the file browser, select all files to be sent in one operation according to the contents of the set:
 - One *.pfx file, or
 - > Two files: one *.pfx file and certPassword.txt, or
 - Three files:pkey.pem, cert.pem and certPassword.txt
- 4 Click Open.

The selected file(s) appear in the *Install Files* path.

- 5 Click Install.
 - The files are sent to the Collaboration Server and the Install File dialog box closes.
- 6 In the Default IP Service Networking IP dialog box, click **OK**.
- 7 In the Reset Confirmation dialog box, click **No** to modify the required system flags before resetting the MCU, or click **Yes** if the flag was already set.



Reset can be performed after setting the system flags (for example, setting the MS_ENVIRONMENT flag). After system reset the Collaboration Server can register to the OCS server and make SIP calls. Sometimes the system fails to read the *.pfx file and the conversion process fails, which is indicated by the active alarm "SIP TLS: Registration server not responding" and/or "SIP TLS: Registration handshake failure". Sending *.pfx file again, as described in this procedure and then resetting the system may resolve the problem.

Collaboration Server System Flag Configuration

Enabling the Microsoft Environment

The Collaboration Server can be installed in Microsoft R2 environments. To adjust the Collaboration Server behavior to the Microsoft environment in each release, system flags must be set.

To configure the system flags on the Polycom Collaboration Server system:

- 1 On the Collaboration Server menu, click Setup > System Configuration. The System Flags - MCMS_PARAMETERS_USER dialog box opens.
- 2 Scroll to the flag MS_ENVIRONMENT and click it. The Edit Flag dialog box is displayed.
- 3 In the Value field, enter YES to set the Collaboration Server SIP environment to Microsoft solution.



Collaboration Server set to MS_ENVIRONMENT=YES supports SIP over TLS only and not over TCP.

- 4 Click **OK** to complete the flag definition.
- 5 When prompted, click **Yes** to reset the MCU and implement the changes to the system configuration. After system reset the Collaboration Server can register to the OCS server and make SIP calls.



Sometimes the system fails to read the *.pfx file and the conversion process fails, which is indicated by the active alarm "SIP TLS: Registration server not responding" and/or "SIP TLS: Registration handshake failure". Sending *.pfx file again, as described in this procedure and then resetting the system may resolve the problem.

In some configurations, the following flags may require modifications when **MS_ENVIRONMENT** flag is set to YES:

Additional MS Environment Flags in the Collaboration Server MCMS_PARAMETERS_USER Tab

Flag Name	Value and Description
SIP_FREE_VIDEO_RESOURCES	Default value in Microsoft environment: NO.
	When set to NO, video resources that were allocated to participants remain allocated to the participants as long as they are connected to the conference even if the call was changed to audio only. The system does not allocate the resources to other participants ensuring that the participants have the appropriate resources in case they want to return to the video call.
	The system allocates the resources according to the participant's endpoint capabilities, with a minimum of one CIF video resource. When this flag is set to YES, video ports are dynamically allocated or released according to the in the endpoint capabilities. For example, when an audio Only call is escalated to Video and vice versa or when the resolution is changed.
SIP_FAST_UPDATE_INTERVAL_ENV	Default setting is 0 to prevent the Collaboration Server from automatically sending an Intra request to all SIP endpoints.
	Enter n (where n is any number of seconds other than 0) to let the Collaboration Server automatically send an Intra request to all SIP endpoints every n seconds.
	It is recommended to set the flag to 0 and modify the frequency in which the request is sent at the endpoint level (as defined in the next flag).
SIP_FAST_UPDATE_INTERVAL_EP	Default setting is 0 to prevent the Collaboration Server from automatically sending an Intra request to Microsoft OC endpoints only, every 6 seconds.
	Enter the number of seconds in which the Collaboration Server automatically sends Intra requests to Microsoft OC endpoints only.

Setting the audio protocol for the Microsoft Client running on a single core PC

By default, Microsoft Office Communicator R2 or Lync Clients are connected to conferences using the G.722.1 audio algorithm. However, when these clients are hosted on single processor workstations, they may experience audio quality problems when this algorithm is used.

The System Flag FORCE_AUDIO_CODEC_FOR_MS_SINGLE_CORE is used to force the use of a specific Audio algorithm such as G.711 when a Microsoft Office Communicator R2 or Lync Client is detected as being hosted on a single core processor.

This flag can be set to:

- AUTO No forcing occurs and the Collaboration Server negotiates a full set of Audio algorithm during capabilities exchange.
- **G711A/U** or **G722** Set this flag value according to the hosting workstation capabilities. If the Collaboration Server detects single core host during capabilities exchange it will assign a *G.711* or *G.722* Audio algorithm according to the flag value.

Possible values: AUTO, G711A, G711U, G722

Default: G711A

Microsoft RTV Video Protocol Support in CP Conferences

Microsoft RTV (Real Time Video) protocol provides high quality video conferencing capability to Microsoft OC (Office Communicator) Client endpoints at resolutions up to HD720p30. Interoperability between Polycom HDX and OCS endpoints is improved.

Guidelines

- The RTV protocol is supported:
 - > In SIP networking environments only
 - > In CP mode only
- OCS (Wave 13) and Lync Server (Wave 14) clients are supported.
- RTV is supported in Basic Cascade mode.
- RTV is the default protocol for OCS endpoints and Lync Server clients connecting to a conference.
- RTV participants are supported in recorded conferences.
- RTV participant encryption is supported using the SRTP protocol.
- Video Preview is not supported for RTV endpoints.
- Custom Slides in IVR Services are not supported for RTV endpoints.
- HD720p30 resolution is supported at bit rates greater than 600 kbps. The following table summarizes
 the resolutions supported at the various bit rates.

RTV - Resolution by Bit Rate

Resolution	Bitrate
QCIF	Bitrate <180kbps
CIF30	180kbps < Bitrate < 250kbps
VGA (SD30)	250kbps < Bitrate < 600kbps *
HD720p30	600kbps < Bitrate *

^{*} Dependant on the PC's capability

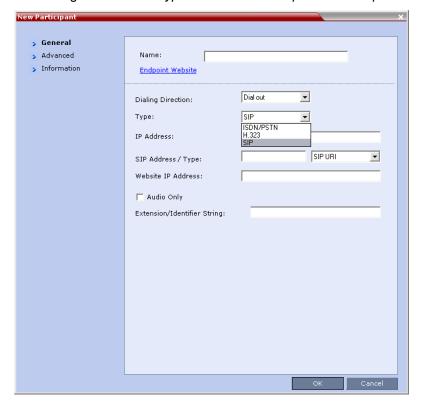
• System Resource usage is the same as for the *H.264* protocol. The table below summarizes System Resource usage for each of the supported resolutions.

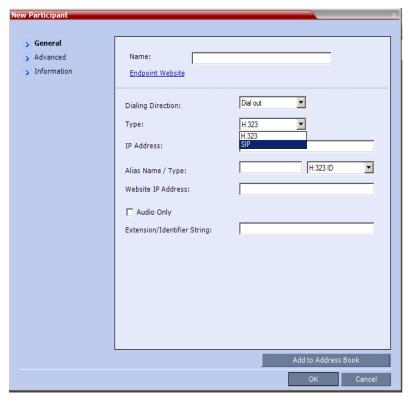
RTV - Resolution by Resolution

Resolution	HD Video Resources Used
QCIF / CIF30	0.333
VGA (SD30) / W4CIF	0.5
HD720p30	1

Participant Settings

When defining a new participant or modifying an existing participant, select **SIP** as the participant's networking environment *Type* in the *New Participant or Participant Properties - General* tab.





The participants *Video Protocol* in the *New Participant or Participant Properties - Advanced* tab should be left at (or set to) its default value: **Auto**.

The **Auto** setting allows the video protocol to be negotiated according to the endpoint's capabilities:

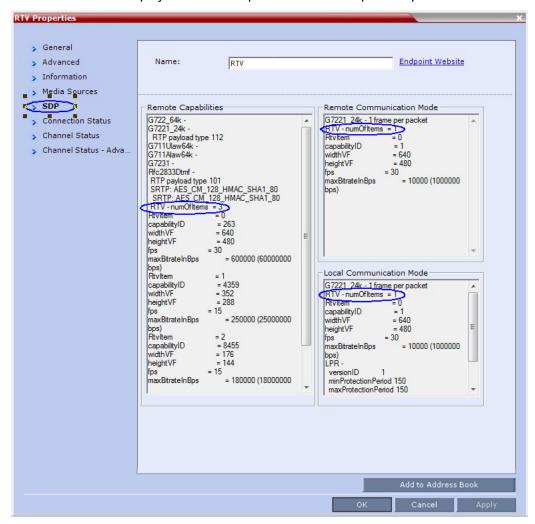
- OCS endpoints and Lync Server clients connect to the conference using the RTV protocol.
- Other endpoints negotiate the video protocol in the following sequence: *H.264*, followed by *RTV*, followed by *H.263* and finally *H.261*.

Protocol Forcing

Selecting *H.264*, *RTV*, *H.263* or *H.261* as the *Video Protocol* results in endpoints that do not support the selected *Video Protocol* connecting as *Secondary* (audio only).

Monitoring RTV

RTV information is displayed in all three panes of the Participant Properties - SDP tab.



Controlling Resource Allocations for Lync Clients Using RTV Video Protocol

The number of resources used by the system to connect a Lync client with RTV is determined according to the conference line rate and the Maximum video resolution set in the *Conference Profile*.

In versions 7.6 and earlier, when conferences are set to line rates above 600 kbps, the Collaboration Server could allocate up to three video resources to Lync clients connecting using the RTV video protocol.

From version 7.6.1, the The system flag **MAX_RTV_RESOLUTION** enables you to override the Collaboration Server resolution selection and limit it to a lower resolution. Resource usage can then be minimized the 1 or 1.5 video resources per call instead of 3 resources, depending on the selected resolution. Possible flag values are: **AUTO** (default), **QCIF**, **CIF**, **VGA** or **HD720**.

For example, if the flag is set to VGA, conference line rate is 1024Kbps, and the Profile Maximum Resolution is set to Auto, the system will limit the Lync RTV client to a resolution of VGA instead of HD720p and will consume only 1.5 video resources instead of 3 resources.

When set to **AUTO** (default), the system uses the default resolution matrix based on the conference line rate.

To change the default flag setting, add the MAX_RTV_RESOLUTION flag to the *System Configuration flags* and set its value. For information, see the *RealPresence Collaboration Server 800s Administrator's Guide*, the *RealPresence Collaboration Server 800s Administrator's Guide*, Modifying System Flags.

The following table summarizes the Collaboration Server resources allocated to a Lync Client based on the MAX_RTV_RESOLUTION flag setting, the connection line rate and the video resolution.

Selected video resolution based on flag setting and conference line rate and core processor

Maximum Resolution Value	Line Rate	Selected Video F	Selected Video Resolution Per Core Processor		
	Line Rate	Quad	Dual	Single	
AUTO	> 600 kbps	HD720p 30fps	VGA 30fps	VGA 15fps	
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps	
	180 kbps - 249 kbps	CIF	CIF	CIF	
	64 kbps - 179 kbps	QCIF	QCIF	QCIF	
HD720p	> 600 kbps	HD720p 30fps	HD720p 13fps	VGA 15fps	
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps	
	180 kbps - 249 kbps	CIF	CIF	CIF	
	64 kbps - 179 kbps	QCIF	QCIF	QCIF	
VGA	> 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps	
	250 kbps - 600 kbps	VGA 30fps	VGA 30fps	VGA 15fps	
	180 kbps - 249 kbps	CIF	CIF	CIF	
	64 kbps - 179 kbps	QCIF	QCIF	QCIF	
CIF	> 600 kbps	CIF	CIF	CIF	
	250 kbps - 600 kbps	CIF	CIF	CIF	
	180 kbps - 249 kbps	CIF	CIF	CIF	
	64 kbps - 179 kbps	QCIF	QCIF	QCIF	
QCIF	> 600 kbps	QCIF	QCIF	QCIF	
	250 kbps - 600 kbps	QCIF	QCIF	QCIF	
	180 kbps - 249 kbps	QCIF	QCIF	QCIF	
	64 kbps - 179 kbps	QCIF	QCIF	QCIF	



When the MAX_ALLOWED_RTV_HD_FRAME_RATE flag equals 0 (default value), Table 1-1 for the MAX_RTV_RESOLUTION flag applies. When the MAX_ALLOWED_RTV_HD_FRAME_RATE flag does not equal 0.

The following table describes the number of allocated video resources for each video resolution when using the RTV protocol.

Allocated video resolutions per video resolution

Selected Video Resolution	Number of Allocated Video Resources
HD720p	3
VGA	1.5
CIF	1
QCIF	1

Threshold HD Flag Settings using the RTV Video Protocol

The system flag **MAX_ALLOWED_RTV_HD_FRAME_RATE** defines the threshold Frame Rate (fps) in which RTV Video Protocol initiates HD resolutions.

Flag values are as follows:

• Default: 0 (fps) - Implements any Frame Rate based on Lync RTV Client capabilities



If the MAX_RTV_RESOLUTION flag is set to AUTO dual core systems always view VGA. For more information on Lync RTV Client capabilities, see , Controlling Resource Allocations for Lync Clients Using RTV Video Protocolfor more information.

• Range: 0-30 (fps)

For example, when the flag is set to 15 and the Lync RTV Client declares HD 720P at 10fps, because the endpoint's frame rate (fps) of 10 is less than flag setting of 15, then the endpoint's video will open VGA and not HD.

In another example, when the flag is set to a frame rate of 10 and the Lync RTV Client declares HD 720P at 13fps, because the endpoint's frame rate (fps) of 13 is greater than flag setting of 10, then the endpoint's video will open HD and not VGA



- Single core PC's cannot view HD and always connect in VGA.
- Dual Core Processor The threshold for flag settings on Dual Core systems is 13 (fps) and less for viewing HD. When system flag is set to 14 (fps) or higher, the RTV Video Protocol shall connect in VGA.
- Quad Core PC systems always view HD, even when flag settings are set anywhere from to 0-30.
- The number of resources used by the system to connect a Lync client with RTV is determined according to the conference line rate and the maximum video resolution set in the Conference Profile.

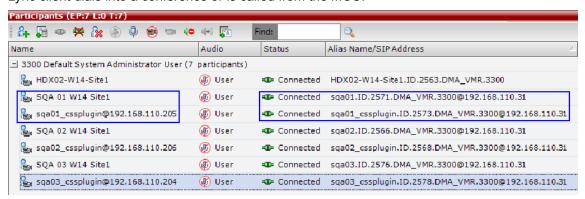
Sharing Content via the Polycom CSS Plug-in for Lync Clients

From version 8.1, Polycom CSS (Content Sharing Suite) Plug-in for Lync clients allows Lync clients to receive and send *Content* on a separate channel, without having to use the video channel. *Content* is transmitted using SIP BFCP.

When Lync clients connect, each endpoint is represented twice in the *RMX Manager* or *Collaboration Server Web Client*. One connection represents the actual Lync client, while the second connection represents the content channel via the Polycom plug-in.

The name of the plug-in "participant" is derived from the name of the Lync client with the suffix "_cssplugin".

When a Lync client connects to a conference, the plug-in connects automatically, regardless of whether the Lync client dials into a conference or is called from the MCU.



Guidelines

- The maximum resolution for content sharing via the Polycom CSS plug-in is HD720p5.
- The Polycom CSS plug-in supports H.263 and H.264 video protocols for content sharing.
- SVC-enabled endpoints use the AVC (H.264) protocol for sharing content.
- Content can be shared between different types of endpoints, using different network protocols (H.323, SIP and ISDN/PSTN).
- TIP content is not supported.
- Lync 2013 is supported.
- ICE is not supported.

Configuring the MCU for Content Sharing via the Polycom CSS Plug-in

You can configure the MCU for content sharing via the Polycom CSS plug-in by setting the following parameters:

- Setting the BLOCK_CONTENT_LEGACY_FOR_LYNC system flag
- Setting the Content parameters in the conference Profile

Setting the System Flag

By configuring the system flag **BLOCK_CONTENT_LEGACY_FOR_LYNC** you control the system behavior in an environment where some Lync clients use the Polycom CSS plug-in and some do not. This flag must be manually added to the system configuration to change its value.

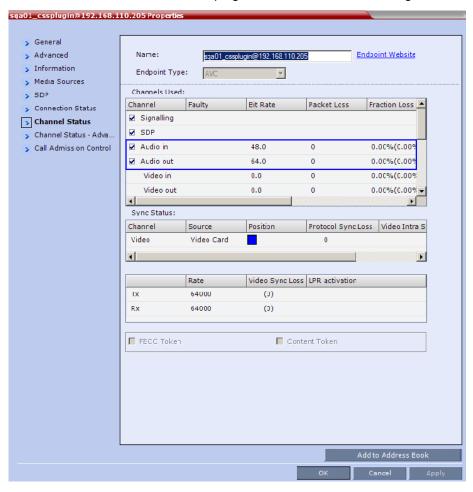
- When set to NO (default), Content is sent to all Lync clients over the video channel, including those
 with the Polycom CSS plug-in installed, even when the Send Content to Legacy Endpoints is
 disabled.
 - Other, non-Lync legacy endpoints will not be affected by this flag and will receive content according to the *Send Content to Legacy Endpoints* settings in the conference *Profile*.
- When set to YES, Content is not sent to Lync clients over the video channel including those with the Polycom CSS plug-in installed, even when the Send Content to Legacy Endpoints is enabled. Other, non-Lync legacy endpoints will not be affected by this flag and will receive content according to the Send Content to Legacy Endpoints settings in the conference Profile.

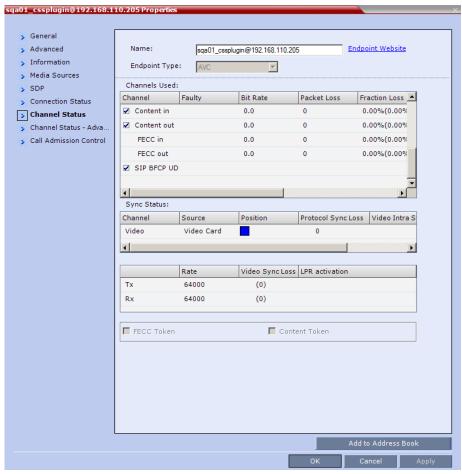
Conference Profile Settings

Content is shared in a video switching mode. Therefore, when a Lync client connects to the conference via the Polycom CSS plug-in, the content resolution will be adjusted to the maximum content rate possible by the Lync client, up to a maximum of **720p 5fps** in all line rates, even if you select a higher content rate and resolution in the *Conference Profile*.

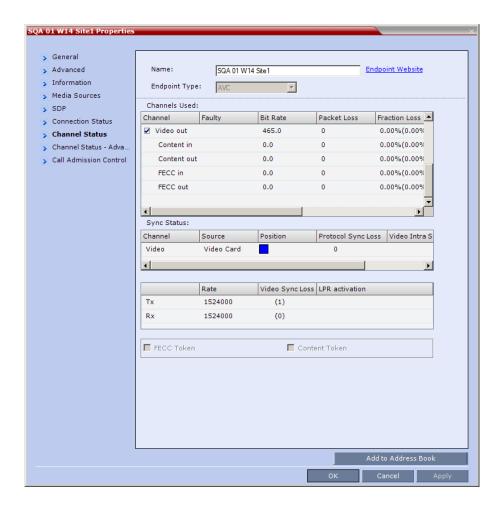
Monitoring the Participant connection

• Under properties of the participant representing the CSS plug-in, *Channel Status*, audio channels are shown, but audio is not used in the plug-in. The information can be ignored.





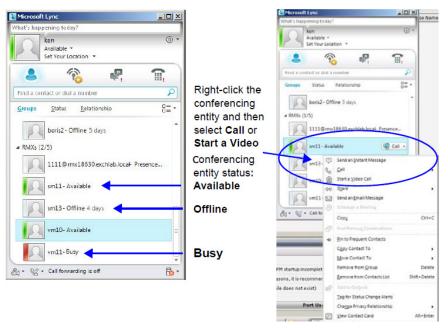
• The properties of the Lync client are those of a video participant. However, the *Content* channel will show 0 as there is no content channel.



Adding Presence to Conferencing Entities in the Buddy List

Registration of conferencing entities (Meeting Rooms, Entry Queues and SIP Factories) with the SIP server adds these conferencing entities to the buddy list with their presence. It enables the Office Communication

Server client or LYNC Server client users to see the availability status (Available, Offline, or Busy) of these conferencing entities and connect to them directly from the buddy list.



Guidelines

- Registration with Presence of up to 100 conferencing entities to a single SIP Server is supported.
 When this number is exceeded, the additional conferencing entity may appear to be successfully registered but the presence status will be shown as 'Offline' in Lync for any entities beyond the limit.
- Lync endpoints cannot connect to conferencing entities that their presence is "offline".
- The Conferencing Entity: Meeting Room, Entry Queue, SIP Factory (Routing Name) has to be added to the Active Directory as a User.
 - Make sure that a unique name is assigned to the conferencing entity and it is not already used for another user account in the Active Directory.
- The conferencing entity name must not include any upper case letters or special characters: @ #\$ % ^ & * () _ = + | } { : " \] [; / ? > < , . (space) ~.
- When the MCU system is shutting down while a Meeting Room is still active, as indicated by its
 presence, the status remains active for 10 minutes during which Lync endpoints cannot connect to
 the Meeting Room. After 10 minutes, the Meeting Room Status changes to "offline".
- From Version 7.1, registration of the conferencing entity is defined in the Conference Profile (and not in the IP Network Service), enabling you to choose the conferencing entity to register.
- In Multiple Networks configuration, an IP Network Service that is enabled for registration in a Conference Profile cannot be deleted.
- Upgrading from previous versions to version 7.1 and later requires manual update of the registration in the Conference Profiles that are assigned to the conferencing entities.

Enabling the Registration of the Conferencing Entities

The creation of the various conferencing entities is described in the following chapters:

- Meeting Rooms
- Entry Queues, Ad Hoc Conferences and SIP Factories

Registration with presence of conferencing entities with the SIP Server is enabled by performing the following processes:

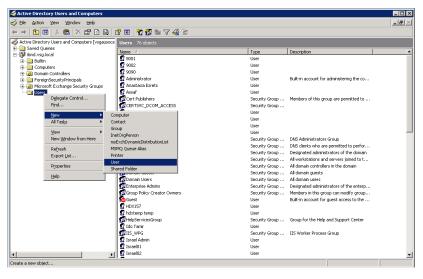
- Creating an Active Directory Account for the Conferencing Entity.
- Enabling the Conferencing Entity User Account for Office Communication Server or Lync Server
- Defining the Microsoft SIP Server in the IP Network Service
- Enabling Registration in the Conference Profile

Creating an Active Directory Account for the Conferencing Entity

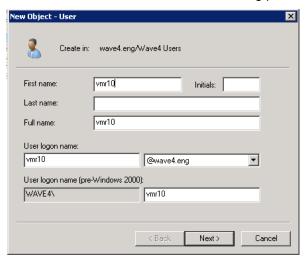
The User account created for the Conferencing entity is used for registration with the Office Communication Server or Lync server and to automatically synchronize with the STUN and relay (Edge) servers.

To add the conferencing entity user to the Active Directory:

- 1 Go to **Start > Run** and enter **dsa.msc** to open the *Active Directory Users and Computers* console.
- 2 In the console tree, select Users > New > User.



3 In the New User wizard, define the following parameters:



Active Directory - New User Parameters for the Collaboration Server

Field	Description	
First Name	Enter the name of the conferencing entity user. This name will appear in the buddy list of the Office Communication Server or Lync server. For example, vmr10. Notes:	
	 This name must be the identical to the Routing Name assigned to the conferencing entity in the Collaboration Server system. It must also be the User Login Name in the Active Directory. The name can include only lower case characters and/or numbers. 	
Full Name	Enter the same name as entered in the First Name field.	
User Login Name	Enter the same name as entered in the <i>First Name</i> field and select from the drop down list the domain name for this user. It is the domain name defined for the Office Communication Server or Lync server.	

- 4 Click Next.
- **5** Enter the password that complies with the Active Directory conventions and confirm the password.
- 6 Select the options: **User cannot change password** and **Password never expires**. Clear the other options.
- 7 Click Next.

The system displays summary information.

8 Click Finish.

The new User is added to the Active Directory Users list.

9 Repeat for each Collaboration Server conferencing entity.

Enabling the Conferencing Entity User Account for Office Communication Server or Lync Server

The new Conferencing Entity user must be enabled for registration with the Office Communications Server or Lync Server.

To enable the Conferencing Entity User Account for Office Communication Server:

- 1 In the *Active Directory Users and Computers* window, right-click the conferencing entity user and then click **Properties**.
- 2 In the *Properties* dialog box, click the **Communications** tab.
- 3 In the Sign in name field, enter the conferencing entity user name in the format SIP:conferencing entity user name (for example sip:vm10) and select the domain name (for example, lab.vsg.local) as entered in the New User dialog box.
- 4 Select the Server or Pool from the list.
- 5 Click **Apply** and then **OK**.

To enable the Conferencing Entity User Account for Lync Server:

1 On the computer running the Lync Server 2010, go to Start->All Programs->Microsoft Lync Server 2010>Lync Server Control Panel.

Windows Security window opens.

- **2** Enter your User name and Password as configured in the Lync Server and click OK. The *Microsoft Lync Server 2010 Control Panel* window opens.
- Click the Users tab.
- 4 In the *User Search* pane, click the **Enable Users** heading.

The New Lync Server User pane opens.

5 Click the Add button.

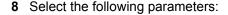
The Select from Active Directory dialog box opens.

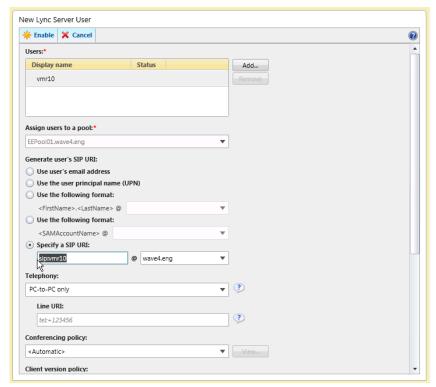
6 Enter the conferencing entity user name as defined in the Active Directory, and then click the Find button.

The requested user is listed in the Select From Active Directory dialog box.

7 Select the listed user (conferencing entity user) and click **OK**.

The selected user is displayed in the New Lync Server User pane.





- In Assign users to a pool field, select the required pool.
- ➤ In the *Generate user SIP URI*, define the SIP URI of the conferencing entity using one of the following methods:
 - Select the Specify a SIP URI option and enter the conferencing entity user portion of SIP URI defined in the active directory. This SIP URI must match the conferencing entity Routing Name configured in Collaboration Server. For example, for the meeting room account sip:vmr10@wave4.eng, use only the vmr10 portion of the address.

or

- ♦ Select the **Use the user principal name (UPN)** option.
- 9 Click the Enable button. The selected user is displayed as enabled in the *User Search* pane.

Defining the Microsoft SIP Server in the IP Network Service

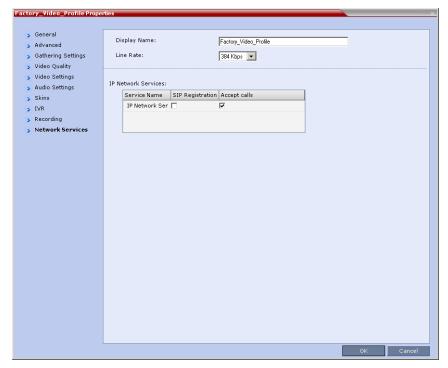
To enable the registration of the conferencing entities the SIP Server Type must be set to **Microsoft** and the Office Communication Server or Lync Server properties in the IP Network Service - SIP Servers dialog box.

For more details, see Configuring the Collaboration Server IP Network Service.

Enabling Registration in the Conference Profile

Registration of conferencing entities such as ongoing conferences, *Meeting Rooms, Entry Queues, SIP Factories* and *Gateway Sessions* with *SIP* servers is done per conferencing entity. This allows better control on the number of entities that register with each *SIP* server.

Selective registration is enabled by assigning a conference Profile in which registration is enabled to the conferencing entities that require registration. Assigning a conference Profile in which registration is disabled (registration check box is cleared) to conferencing entities will prevent them from registering. By default, Registration is disabled in the Conference Profile, and must be enabled in Profiles assigned to conferencing entities that require registration.



Profile Properties - Network Services

Parameter	Description		
IP Network Services	s:		
Service Name	This column lists all the defined <i>Network Services</i> , one or several depending on the system configuration (single Network or Multiple Networks).		
SIP Registration	To register the conferencing entity to which this profile is assigned, with the SIP Server defined for that <i>Network Service</i> , click the <i>SIP Registration</i> check box of that <i>Network Service</i> .		
Accept Calls	To prevent dial in participants from connecting to a conferencing entity when connecting via a certain <i>Network Service</i> , clear the <i>Accept Calls</i> check box of that <i>Network Service</i> .		

Verifying the Collaboration Server Conferencing Entity Routing Name and Profile

Collaboration Server conferencing entity can be dialed directly from the buddy list of the Office Communications client or the Lync client if its routing name matches the user name of Active Directory account you created and Registration is enabled in the Conference Profile assigned to it.

• To ensure that the Collaboration Server meeting room or conferencing entity is properly configured for registration the following parameters must be defined:

> The user name on the conferencing entity in Active Directory account must be identical to its **Routing Name** on the Collaboration Server.

For example, if the SIP URI in the Active Directory is **sip:vmr10@wave4.eng**, it must be defined as **vmr10** in the *Routing Name* field of that Collaboration Server conferencing entity.



In the **Profile** field, make sure that a conference Profile that has been enabled for SIP registration is selected.

Monitoring the Registration Status of a Conferencing Entity in the Collaboration Server Web Client or RMX Manager Application

The Status of the SIP registration can be viewed in the appropriate conferencing Entity list or when displaying its properties.

Conferencing Entity List

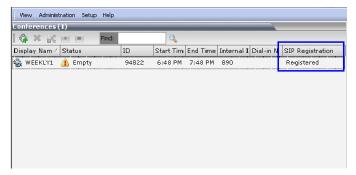
The list of conferencing entity includes an additional column - *SIP Registration*, which indicates the status of its registration with the SIP server. The following statuses are displayed:

Not configured - Registration with the SIP Server was not enabled in the Conference Profile
assigned to this conferencing Entity. In Multiple Networks configuration, If one service is not
configured while others are configured and registered, the status reflects the registration with the
configured Network Services. The registration status with each SIP Server can be viewed in the
Properties - Network Services dialog box of each conferencing entity.

When SIP registration is not enabled in the conference profile, the Collaboration Server's registering to SIP Servers will each register with an URL derived from its own signaling address. This unique URL replaces the non-unique URL, dummy_tester, used in previous versions.

- Failed Registration with the SIP Server failed.
 This may be due to incorrect definition of the SIP server in the IP Network Service, or the SIP server may be down, or any other reason the affects the connection between the Collaboration Server or the SIP Server to the network.
- **Registered** the conferencing entity is registered with the SIP Server.
- Partially Registered This status is available only in Multiple Networks configuration, when the
 conferencing entity failed to register to all the required Network Services (if more than one Network
 Service was selected for Registration). The registration status with each SIP Server can be viewed
 in the Properties Network Services dialog box of each conferencing entity.

Ongoing Conferences list - SIP Registration



Meeting Rooms list - SIP Registration



Entry Queues list - SIP Registration



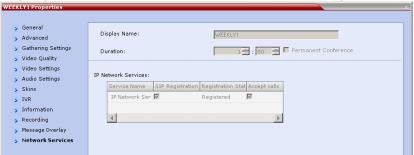
SIP Factories list - SIP Registration



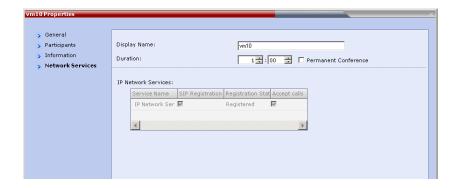
Conferencing Entity Properties

Registration status is reflected in the *Properties - Network Services* dialog box:

Ongoing conference Properties - Network Services - SIP Registration



Meeting Room Properties - Network Services - SIP Registration



Entry Queue Properties - Network Services - SIP Registration



Collaboration Server Configuration for CAC Implementation

CAC is enabled by manually adding the flags to the system Configuration and setting their values as follows:

- To enable the Call Admission Control implementation in the Collaboration Server:
 - CAC_ENABLE=YES
- In addition, to ensure that endpoints such as HDX remain connected to the conference for its duration
 when the Collaboration Server is configured with FQDN address and the Lync server is working with
 load balancing and holds more than one address, the following two flags must be manually added
 and set to:
 - ➤ MS KEEP ALIVE ENABLE = YES

Note: Since the keep alive is only required when the Lync server is working with load balancing and holds more than one address, the default value is NO.

SIP_TCP_PORT_ADDR_STRATEGY = 1 (default setting)

- When Call Admission Control is enabled in the local network, by default the local the ICE channel is closed after applying CAC bandwidth management.
 To change and preserve the ICE channel open throughout the call:
 - > PRESERVE_ICE_CHANNEL_IN_CASE_OF_LOCAL_MODE=YES.

Conferencing Behavior

Continuous Presence Conferences

In Continuous Presence conference, Lync clients connect with any allocated bandwidth.

Video Switching Conferences

In Video Switching conferences, Lync clients must connect with the same line rate as the conference, otherwise they will be connected as Secondary (Audio Only) participants.

Mitigation of the line rate requirement can be effected by modifying the system flag:

VSW_RATE_TOLERANCE_PERECENT.

This system flag determines the line rate tolerance.

Possible values are: 0 - 75.

Setting this flag to **0** (0% - default) determines no line rate tolerance and the participant must connect at the conference line rate.

Setting this flag to a value between 1 and 75 determines the percentage of bandwidth that can be deducted from the required bandwidth to allow participants to connect to the conference.

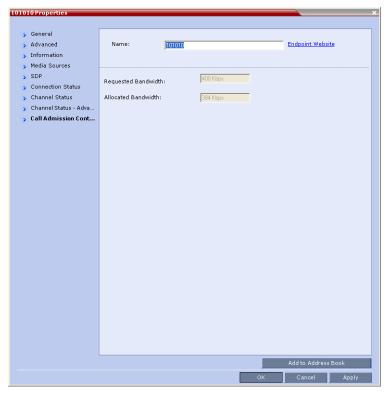
For example, if you enter 20 (for 20%) as the flag value, the participant will be able to connect to the conference if the allocated line rate is up to 20% lower than the conference line rate (or between 80% to 100% of the required bandwidth). If the conference line rate is 1024Kbps, participant with a line rate between 819Kbps and 1024Kbps will be able to connect to the conference.

When a tolerance is set, the Highest Common mechanism is enabled for the conference line rate. When a participant with a lower line rate connects to the conference, the line rate of all other connected participants is reduced accordingly and when that participant disconnects from the conference, the line rate of the remaining participants is increased to the highest possible rate common to all connected participants.

For example, if a participant with a line rate of 900Kbps connects to the conference to which all other participants are connected at a line rate of 1024kbps, the line rate of all participants will decrease to 900Kbps. When this participant disconnects, the line rate of the remaining participants will increase to 1024Kbps.

Monitoring Participant Connections

Activation of the Call Admission Control for a call can be viewed in the *Participant Properties - Call Admission Control* dialog box.



This information applies only to dial-in participants.

The following information is available:

Participant Properties - Call Admission Control Parameters

Field	Description
Requested Bandwidth	Indicates the bandwidth requested by the Lync client (usually the line rate set for the conference). NA - indicates that Call Admission Control is disabled.
Allocated Bandwidth	The actual bandwidth allocated by the Lync Policy Server. NA - indicates that Call Admission Control is disabled.

Connecting a Collaboration Server Meeting Room to a Microsoft AV-MCU Conference

Microsoft Lync users can connect an Collaboration Server Meeting Room to a conference running on the Microsoft A/V MCU. This allows Collaboration Server Lync users to connect with a conference in progress on the A/V MCU and be an active participant in the conference. The connection to the A/V MCU is the same configuration as a cascading conference between multiple Collaboration Server MCUs.

To connect to an A/V MCU conference:

1 From the Menu bar, click **Meet Now** to create an ad-hoc conference. The Group Conversation dialog box is displayed.



2 From the Contacts List on Lync, drag a Virtual Meeting Room (VMR) into the Group Conversation list

After the Virtual Meeting Room is connected on Lync, an invitation is sent from the A/V MCU to the Collaboration Server using the Centralized Conference Control Protocol (CCCP). The Collaboration Server responds and triggers a standard SIP invite sent from the A/V MCU to the Collaboration Server.

Multiple participants can now connect to both the Collaboration Server Meeting Room and the A/V MCU, and participate in a cascaded conference.



When a conference begins with Audio Only, a Lync user cannot add video to the conference after the VMR is connected to the conference. The conference will remain as Audio Only.

Configuring the Collaboration Server for Federated (ICE) Dialing

The Collaboration Server *Default IP Network Service* must be configured to work with the Office Communication Server/Lync Server as the SIP Server and the Collaboration Server user defined in the Active Directory must also be defined in the Collaboration Server ICE environment parameters to enable remote dialing in a federated (ICE) environment, .

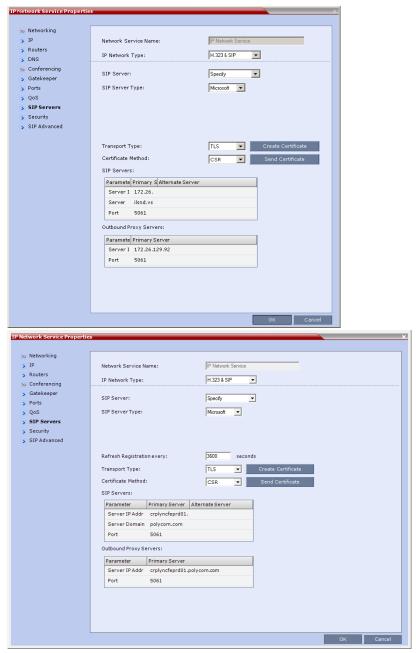


The procedure described here assumes that the Collaboration Server is configured to work in Microsoft environment as described in Configuring the Collaboration Server for Microsoft Integration.

To configure the Collaboration Server for ICE Dialing:

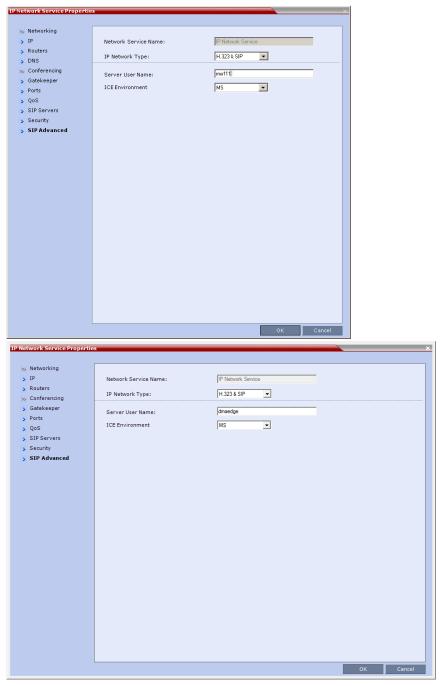
- 1 In the RealPresence Collaboration Server Web browser, in the *RealPresence Collaboration Server RMX Management* pane, expand the **Rarely Used** list and click **IP Network Services**.
- 2 In the *IP Network Services* pane, double-click the **Default IP Service** entry. The *Default IP Service Networking IP* dialog box opens.

3 Click the SIP Servers tab.



- 4 Make sure that the SIP Server is set to Specify.
- **5** Make sure that the SIP Server Type is set to **Microsoft**.
- **6** Make sure that the IP address of the Office Communications Server 2007 or Lync Server 2010 is specified and the *Server Domain Name* is the same as defined in the OCS/Lync Server and in the *Management Network* for the DNS.

7 Click the SIP Advanced tab.



- 8 In the *ICE Environment* field, select **MS** (for Microsoft ICE implementation) to enable the ICE integration.
- 9 In the Server User Name field, enter the Collaboration Server User name as defined in the Active Directory. For example, enter rmx111.
 This field is disabled if the ICE Environment field is set to None.

- 10 Optional if the Fixed Ports options was selected previously.
 Click the Ports tab to modify the number of UDP Ports allocated to the calls to accommodate the number of ports required for ICE dialing.
- 11 In the *UDP Port Range*, modify the number of UDP ports by enter the first and last port numbers in the range. When ICE environment is enabled, the number of ports defined in the range should be 2024.
- 12 Click OK.

The Collaboration Server will register with the OCS/Lync Server enabling automatic retrieval of the STUN server and Relay server parameters for ICE dialing.

These parameters can be viewed in the Signaling Monitor - ICE Servers dialog box.

Monitoring the Connection to the STUN and Relay Servers in the ICE Environment

- 1 In the Collaboration Server Web browser, in the Collaboration Server Management pane, click Signaling Monitor.
- 2 In the Signaling Monitor pane, click the IP Network Service entry.
- 3 Click the ICE Servers tab.



The system lists the ICE servers to which it is connected and the status of the connection of each of the Collaboration Server media cards (status 1, status 2, etc) to ICE servers. (One status is displayed for RealPresence Collaboration Server (RMX) 1500, two statuses are displayed for RealPresence Collaboration Server (RMX) 2000 and four statuses are displayed for RealPresence Collaboration Server (RMX) 4000).

It addition, the system indicates the status of the firewall detection in the Collaboration Server.

Monitoring the Participant Connection in ICE Environment

For each participant in the conference running in ICE environment, you can view the local and the external IP addresses and the type of connection between the Collaboration Server and the participant (remote).

The ICE information is displayed only for the media channels and not the signaling channel.

To view the channel properties of the participant:

- 1 In the participants pane, double-click the participant entry or right-click the participant entry and then click **Properties**.
- Click the Channel Status Advanced tab.



The following connection information is displayed:

Participant Properties - ICE Connection Parameters

Field	Description	
Collaboration Server IP Address	The local IP address and port (in the format IP address:Port) of the Collaboration Server.	
Participant IP Address	The local IP address and port (in the format IP address:Port) of the endpoint.	
ICE Collaboration Server IP Address	 The IP address and the Port number of the Collaboration Server used to pass through the media. This information changes according to the ICE connection type: When ICE connection type is local, it is identical to the IP address:Port displayed in the Collaboration Server IP Address. When ICE connection type is relay, the system displays the IP address and port number of the relay server used to pass the media from the Collaboration Server to the participant. When ICE connection type is firewall, the system displays the public IP address and port of the Collaboration Server as seen outside the private 	

Field	Description	
ICE Participant IP Address	 The IP address and the Port number of the endpoint used to pass through the media. This information changes according to the ICE connection type: When ICE connection type is local, it is identical to the IP address:Port displayed in the Participant IP Address. 	
	 When ICE connection type is relay, the system displays the IP address and port number of the relay server used to pass the media from the participant to the Collaboration Server. 	
	 When ICE connection type is firewall, the system displays the public IP address and port of the endpoint as seen outside the private network. 	
ICE Connection Type	Indicates the type of connection between the Collaboration Server and the participant in the ICE environment:	
	 Local (or Host) - The endpoint (Remote) is on the same network as the Collaboration Server and the media connection is direct, using local addresses. 	
	 Relay - Media between the Collaboration Server and the participant passes through a media relay server. 	
	 Firewall - Media connection between the Collaboration Server and the participant is done using their external IP addresses (the IP addresses as seen outside of the local network). 	

For a detailed description of ICE Active alarms, see ICE Active Alarms.

Active Alarms and Troubleshooting

Active Alarms

The following active alarms may be displayed in the Collaboration Server *System Alerts* pane when the Collaboration Server is configured for integration in the OCS environment:

Active Alarms

Alarm Code	Alarm Description
SIP TLS: Failed to load or verify certificate files	This alarm indicates that the certificate files required for SIP TLS could not be loaded to the Collaboration Server. Possible causes are:
	 Incorrect certificate file name. Only files with the following names can be loaded to the system: rootCA.pem, pkey.pem, cert.pem and certPassword.txt
	 Wrong certificate file type. Only files of the following types can be loaded to the system: rootCA.pem, pkey.pem and cert.pem and certPassword.txt
	 The contents of the certificate file does not match the system parameters

Alarm Code	Alarm Description
SIP TLS: Registration transport error	This alarm indicates that the communication with the SIP server cannot be established. Possible causes are: Incorrect IP address of the SIP server The SIP server listening port is other than the one defined in the system The OCS services are stopped Note: Sometimes this alarm may be activated without real cause. Resetting the MCU may clear the alarm.
SIP TLS: Registration handshake failure	This alarm indicates a mismatch between the security protocols of the OCS and the Collaboration Server, preventing the Registration of the Collaboration Server to the OCS.
SIP TLS: Registration server not responding	 This alarm is displayed when the Collaboration Server does not receive a response from the OCS to the registration request in the expected time frame. Possible causes are: The Collaboration Server FQDN name is not defined in the OCS pool, or is defined incorrectly. The time frame for the expected response was too short and it will be updated with the next data refresh. The alarm may be cleared automatically the next time the data is refreshed. Alternatively, the OCS Pool Service can be stopped and restarted to refresh the data. The Collaboration Server FQDN name is not defined in the DNS server. Ping the DNS using the Collaboration Server FQDN name to ensure that the Collaboration Server is correctly registered to the DNS.
SIP TLS: Certificate has expired	The current TLS certificate files have expired and must be replaced with new files.
SIP TLS: Certificate is about to expire	The current TLS certificate files will expire shortly and will have to be replaced to ensure the communication with the OCS.
SIP TLS: Certificate subject name is not valid or DNS failed to resolve this name	This alarm is displayed if the name of the Collaboration Server in the certificate file is different from the FQDN name defined in the OCS. Note: Occasionally this alarm may be activated without real cause. Resetting the MCU may clear the alarm.

ICE Active Alarms

When ICE environment is enabled in the Collaboration Server, failure to communicate with a required component triggers the display of an Active Alarm in the System Alerts pane.

The following table lists these active alarms:

ICE Environment - Collaboration Server Active Alarms

Active Alarm	Phase	Alarm Displayed When	Troubleshooting
ICE failure: Failed to register with OCS. Check the Collaboration Server Server Name.	Registration	The Collaboration Server did not receive a confirmation response from the OCS to the Registration request.	Check that the Collaboration Server Name in IP Network Service - SIP Advanced is identical to the User name defined for the Collaboration Server in the OCS Active Directory. Make sure that the Collaboration Server user is defined in the OCS Active Directory.
ICE failure: Failed to subscribe with the OCS, therefore the A/V Edge Server URI was not received.	Subscribe	The Collaboration Server did not receive a confirmation response from the OCS to the Subscription request. The Subscription is required for obtaining the A/V Edge Server URI which is followed by the notify message containing the credentials).	
ICE failure: The Notify message containing the A/V Edge Server URI was not received	Notify	The Notify message containing the A/V Edge Server URI was not received by the Collaboration Server.	
ICE failure: Received Notification does not contain URI.	Notify	The notify message that was sent from the A/V Edge Server does not contain the A/V Edge server URI.	Verify the A/V Edge server is configured in the OCS.
ICE failure: No response from the A/V Edge Server to the Collaboration Server Service Request	Service	The Collaboration Server did not receive a confirmation response from the A/V Edge Server to the Service request.	
ICE failure: Received Service message does not contain the Credentials.	Service	The Service message response does not contain the Credentials.	
ICE failure: A/V Edge server URI cannot be resolved	Service	The Collaboration Server failed to resolve The remote address of the Edge server URI.	

Active Alarm	Phase	Alarm Displayed When	Troubleshooting
ICE failure: Service credential denied. A/V Edge server credentials rejected by the OCS.	Service	This alarm indicates that the OCS does not configure with the. Generated by the ICE stack.	

Troubleshooting

- At the end of the installation and configuration process, to test the solution and the integration with the OCS, create an ongoing conference with two participants, one dial-in and one dial-out and connect them to the conference.
- If the active Alarm "SIP TLS: Registration server not responding" is displayed, stop and restart the OCS Pool Service.
- If the communication between the OCS and the Collaboration Server cannot be established, one of
 the possible causes can be that the Collaboration Server FQDN name is defined differently in the
 DNS, OCS and Collaboration Server. The name must be defined identically in all three devices, and
 defined as type A in the DNS. The definition of the Collaboration Server FQDN name in the DNS can
 be tested by pinging it and receiving the Collaboration Server signaling IP from the DNS in return.
- The communication between the OCS and the Collaboration Server can be checked in the Logger files:
 - ➤ SIP 401/407 reject messages indicate that the Collaboration Server is not configured as Trusted in the OCS and must be configured accordingly.
 - > SIP 404 reject indication indicates that the connection to the OCS was established successfully.

Known Issues

- Selecting Pause my Video in OC client causes the call to downgrade to audio only call if the call was not in Audio Only mode at all (the call was started as a video call).
 - If the call is started as an audio only call and video is added to it, or if the call was started as video call and during the call it was changed to Audio Only and back to video, selecting *Pause my Video* will suspend it as required.
- Rarely, the OC client disconnects after 15 minutes. The OC client can be reconnected using the same dialing method in which they were previously connected (dial-in or dial-out).
- Rarely, all SIP endpoints disconnect at the same time. The SIP endpoint can be reconnected using the same dialing method in which they were previously connected (dial-in or dial-out).

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners. These additional services will help customers successfully design, deploy, optimize and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. For additional information and details please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Appendix I - Polycom Open Collaboration Network (POCN)



Working in the Open Collaboration Server and TIP protocol are supported in AVC Conferencing Mode only.

Collaboration With Cisco's Telepresence Interoperability Protocol (TIP)

TIP is a proprietary protocol created by Cisco for deployment in Cisco TelePresence systems (CTS). Since TIP is not compatible with standard video communication systems, interoperability between Cisco and other vendors' Telepresence systems was initially impossible.

Gateways were developed to provide interoperability but were subject to the inherent problems of additional latency (delay) in connections and low video quality resulting from the reformatting of video and audio content.

Polycom's solution is to allow the Collaboration Server to natively inter-operate with Cisco TelePresence Systems, ensuring optimum quality multi-screen, multipoint calls between:

- Polycom Immersive Telepresence Systems (ITP) Version 3.1.1:
 - RPX 200
 - RPX 400
 - ➤ OTX 300

(At Telepresence Licence is required on the Collaboration Server.)

- Polycom video conferencing endpoints
 - Standalone HDX
 - Polycom Group Series 300/500
- Microsoft
 - MS Lync (using MS-ICE)
 - ➤ RTV 720p
- Cisco TelePresence® System (CTS) Versions 1.10Collaboration ServerCollaboration ServerCollaboration Server
 - > CTS 1300
 - > CTS 3010

Conferences hosted on the Collaboration Server can include a mix of existing end points (that do not support TIP) and CTS endpoints.

TIP-enabled endpoints must support TIP Version 7 or higher. Calls from endpoints supporting older versions of TIP will be rejected.

Deployment Architectures

The following multipoint topologies are given as examples. Actual deployments will depend on user requirements and available infrastructure:

- Single company with Polycom and Cisco Infrastructure
 - > CTS and Polycom Telepresence Rooms in a corporate environment.
- Company to company via Service Provider
 - > Model 1: Mixed Polycom and Cisco infrastructure at one of the companies, Cisco only infrastructure at the other.
 - Model 2: Polycom only infrastructure at one of the companies, Cisco only infrastructure at the other.

Single Company Model - Polycom and Cisco Infrastructure

The deployment architecture in Single company with Polycom and Cisco Infrastructure - Polycom endpoints using SIP shows a company that has a mixture of Polycom and Cisco endpoints, room systems and telephony equipment that needs to enable multipoint calls between all its video and audio endpoints using the Collaboration Server as the conference bridge.

As shown in Single company with Polycom and Cisco Infrastructure - Polycom endpoints using SIP, prior to Version 8.1.1, Cisco Telepresence endpoints could connect to conferences using the TIP protocol, Polycom endpoints connected to the same conferences using SIP protocol.

Standard Based RTP / RTCP TIP Based RTP / RTCP SIP Signaling H. 323 E1 (PSTN / ISDN) Polycom CMA Polycom H. 323 DMA RPX 4.88 Phone Signaling H. 323 Trunk SIP Trunk SIP Trunk SIP Trunk Cisco IDS Gatekeeper Phone H. 323 Trunk SIP Trunk SIP Trunk SIP Trunk Cisco MCU H. 323 Trunk SIP Trunk SIP Trunk SIP Trunk SIP Trunk Cisco MCU H. 323 Trunk SIP Trunk SIP Trunk Cisco Unified Personal Communicator (SIP) Cisco Unified Personal Communicator (SIP)

Single company with Polycom and Cisco Infrastructure - Polycom endpoints using SIP

Polycom endpoints can also connect to Entry Queues, Meeting Rooms and conferences using all protocols, including TIP and SIP.

Polycom VVX 1500 C SIP Phone

The following table lists components and versions of the Collaboration Server and Cisco Telepresence Systems (CTS) Integration Solution Architecture.

Solution Architecture Components

Component	Version	Description
CISCO Equipment		
CUCM	8.5.1, 8.6.2	Cisco Unified Communication Manager: CUCM must be configured to: Route calls to DMA (if present). Route all H.323 calls to the gatekeeper, which can be either CMA or IOS.
IOS	15.1T	Cisco Internetwork Operating System - Gatekeeper
Endpoints (CTS)	1.7.2 (ATT), 1.8.1	Telephony, desktop and room systems. CTS endpoints must register to CUCM.

Component	Version	Description
Cisco Unified Video Conferencing 5230	7.2	MCU.
Cisco Unified Presence	8.5, 8.6	Network-based Presence and Instant Messaging.
Cisco Unified Contact Center Express	8.0, 8.5	Call distributor (ACD), interactive voice response (IVR) and computer telephony integration (CTI).
Cisco IP Communicator	7.0,8.6	Windows PC-based softphone application.
Cisco Unified Personal Communicator	8.5(2),8.5(5)	Web client for Presence and Instant Messaging.
Cisco Unified Video Advantage	2.2(2)	Video telephony functionality for Cisco Unified IP phones.
Cisco Unified IP Phones 7960, 7961, 7962, 7965, 7975	CUCM 8.5.1 / CUCM 8.6.1 compatible	IP Phones.
Cisco Unified IP Phones 9971	CUCM 8.5 / CUCM 8.6(2) compatible	_
CTMS	1.7.3, 1.8.2	Cisco TelePresence Multipoint Switch.
Cisco Unified Border Element	15.1T	SBC - Voice and video connectivity from enterprise IP network to Service Provider SIP trunks.
Telepresence Server	2.2(1.54)	Telepresence Server.
VCS	X7.1	Video Communication Server / Session Manager.
Polycom Equipment		
DMA 7000	4.0	 Polycom Distributed Media Application DMA is an optional component but is essential if Content sharing is to be enabled. All SIP endpoints register to DMA as a SIP Proxy. DMA should be configured to route SIP calls (with CTS destination) to CUCM. If DMA is not present in the solution architecture, SIP endpoints must register to CUCM as gatekeeper. DMA must be configured with a VMR (Virtual Meeting Room). Incoming calls are then routed to the Collaboration Server.

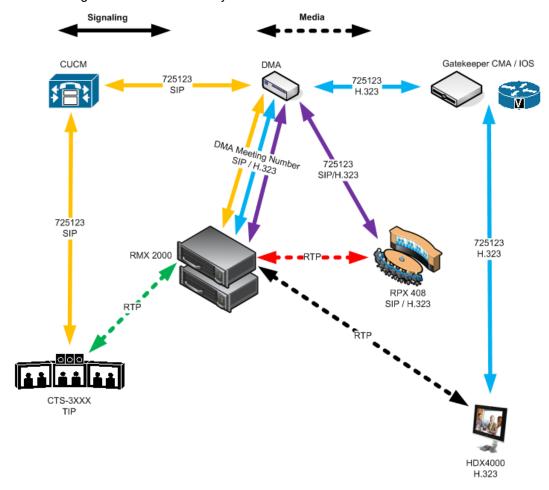
Component	Version	Description
Collaboration Server	7.6 and higher	 MCU: Functions as the network bridge for multipoint calls between <i>H.323</i>, <i>SIP</i> and <i>TIP</i> endpoints. The Collaboration Server can be interfaced to <i>CUCM</i> using a <i>SIP</i> trunk, enabling <i>CTS</i> to join multipoint calls on Collaboration Server. Signaling goes through the <i>CUCM</i> while the media in <i>TIP</i> format goes directly between the <i>CTS</i> and Collaboration Server. The Collaboration Server must be configured to route outbound SIP calls to DMA. The H.323 Network Service of the Collaboration Server should register it's dial prefix with the <i>CMA</i> gatekeeper. When DMA is not used an <i>Ad-hoc Entry Queue</i>, designated as <i>Transit Entry Queue</i>, must be pre-defined on the Collaboration Server.
MLA	3.0.3	Multipoint Layout Application Required for managing multi-screen endpoint layouts for Cisco CTS 3XXX, Polycom TPX, RPX or OTX systems.
CMA	5.5	Polycom Converged Management Application - Gatekeeper The gatekeeper must route calls to Collaboration Server based on the Collaboration Server prefix registration on the gatekeeper.
Endpoints		 Telephony, desktop and room systems. H.323 endpoints must register to the CMA or IOS gatekeeper. Polycom SIP endpoints must register to DMA as SIP Proxy when DMA is used. H.323 endpoints must register to the CMA or IOS gatekeeper.

Call Flows

Multipoint call with DMA

In this example:

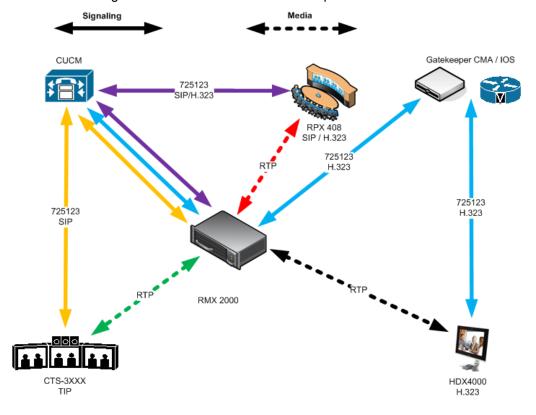
- Collaboration Server prefix in the gatekeeper: 72
- Virtual Meeting Room in DMA: 725123
- DMA Meeting Number: Generated by DMA



Multipoint call without DMA

In this example:

- Collaboration Server prefix in the gatekeeper: 72
- CUCM: According to its Dial Plan forwards calls with prefix 72 to the Collaboration Server



Company to Company Models Using a Service Provider

Using this topology, both companies connect to a Service Provider via a Cisco Session Border Controller (SBC). The Service Provider functions as a B2B Telepresence Exchange, enabling multipoint calls between the two companies and their respective video and audio endpoints using the Collaboration Server as the conference bridge.

The SBC functions as a firewall that the Service Provider can configure according to Trust Relationships between two or several companies. By using this method, companies do not have to open their corporate firewalls and administer connectivity with the many companies they may need to communicate with.

Two topology models are discussed:

- Model 1:
 - Company A has a Polycom only environment.
 - Company B has a Cisco only Environment.
- Model 2:
 - > Company A has a mixed Polycom and Cisco environment.
 - Company B has a Cisco only Environment.

Model 1

The deployment architecture in Call Flow shows two companies: Company A and Company B.

Company A - has deployed a Polycom solution including:

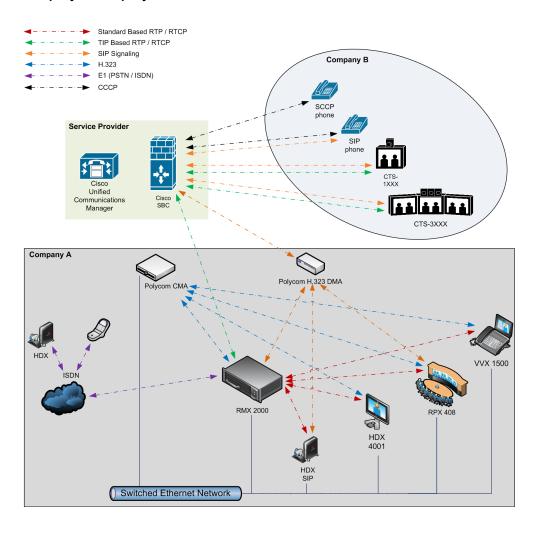
- DMA
- Collaboration Server
- MLA
- CMA Gatekeeper
- Polycom telephony and desktop endpoints.

Company B - has deployed a Cisco solution including:

- CTS 1000
- CTS 3000

• Cisco telephony and desktop endpoints

Company to Company via Service Provider - Model 1

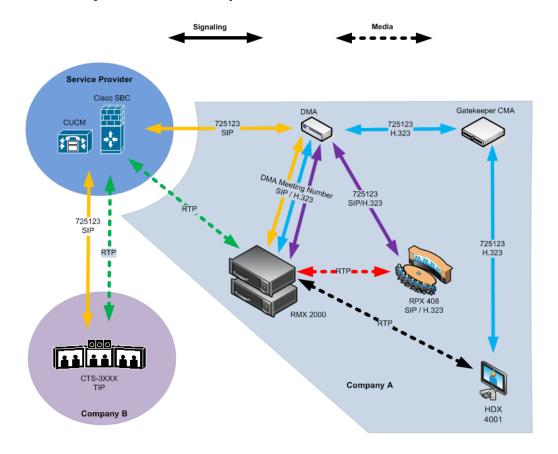


Call Flow

Multipoint call via Service Provider - Model 1

In this example:

- Collaboration Server prefix in the gatekeeper: 72
- Virtual Meeting Room in DMA: 725123
- DMA Meeting Number Generated by DMA



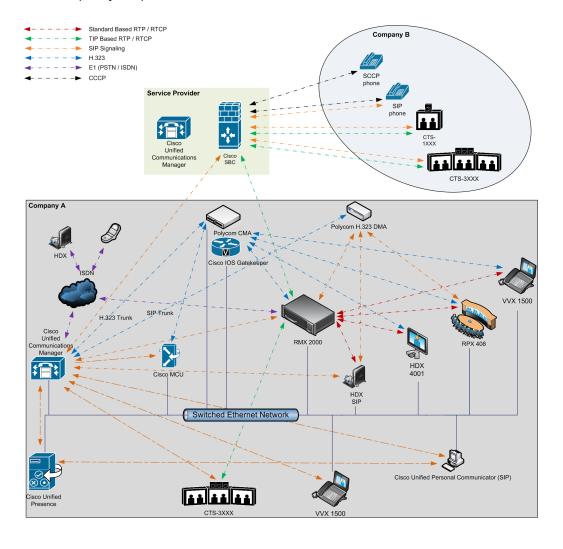
Multipoint call via Service Provider - Model 2

The deployment architecture in *The deployment architecture includes:* shows two companies: *Company A* and *Company B*.

Company A - has the same deployment architecture as shown in *Single Company Model - Polycom and Cisco Infrastructure*.

Company B - has deployed a Cisco solution including:

- CTS 1000
- CTS 3000
- Cisco telephony endpoints.



The deployment architecture includes:

Company A

For a full description of Company A's deployment, see Single Company Model - Polycom and Cisco Infrastructure.

Differing or additional configuration requirements for each element of this deployment model are listed below:

Company A Solution Architecture Components

Component	Version	Description
CISCO Equipment		
CUCM	8.5	Cisco Unified Communication Manager:
		CUCM must be configured with a SIP trunk to the Service Provider's SBC.
Polycom Equipment		
Collaboration Server	7.6.x	MCU:
		Collaboration Server must be configured to send and receive RTP streams to and from the Service Provider's SBC.

Company B

Company B Solution Architecture Components

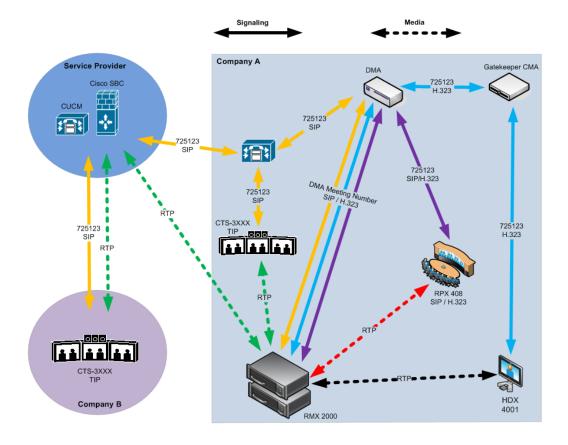
CISCO Equipment	
Endpoints	Endpoints should register with the <i>Service Provider's CUCM</i> (or the local CUCM, if present).

Call Flow

Multipoint call via Service Provider - Model 2

In this example:

- Collaboration Server prefix in the gatekeeper: 72
- Virtual Meeting Room in DMA: 725123
- · CUCM: According to its Dial Plan forwards calls with prefix 72 to the Collaboration Server



Administration

The various deployment combinations and settings within the various Deployment Architectures affects the administration of the system.

Gatekeepers

Standalone Polycom CMA/DMA System as a Gatekeeper

The Polycom CMA/DMA system can be used as the only gatekeeper for the network. Bandwidth and call admission control of endpoints registered with the CMA system is split between the CMA system and the CUCM.

For more information see the Polycom Unified Communications Deployment Guide for Cisco Environments.

Standalone Cisco IOS Gatekeeper

The Cisco IOS Gatekeeper can be used as the only gatekeeper for the network if the management capabilities of the Polycom CMA system are not required.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Neighbored Cisco IOS and Polycom CMA/DMA Gatekeepers

Neighbored gatekeepers make it easier to create a common dial plan and should be considered when integrating an existing Cisco telephony environment with an existing Polycom network. Neighbored Gatekeepers allow number translation while maintaining the existing environments.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*,DMA

The Polycom DMA system can be configured as a SIP proxy and registrar for the environment. When used as a SIP peer, the DMA system can host video calls between Cisco endpoints that are registered with the CUCM and Polycom SIP endpoints that are registered with the DMA system.

For more information see the Polycom Unified Communications Deployment Guide for Cisco Environments.

CUCM

When Polycom SIP endpoints (voice and video) are registered directly with CUCM you can take advantage of supported telephone functions. CUCM may not support the full range of codecs and features available on the Polycom equipment. CUCM supported codecs and features will be used in such cases.

For more information see Polycom Unified Communications Deployment Guide for Cisco Environments.

Configuring the Cisco and Polycom Equipment

MLA (Multipoint Layout Application) is required for managing CTS 3XXX layouts whether Polycom TPX, RPX or OTX systems are deployed or not. MLA is a Windows® application that allows conference administrators to configure and control video layouts for multipoint calls involving Polycom Immersive Telepresence (ITP) systems.

Call Detail Records (CDR) are generated on both the CMA Gatekeeper and the CUCM for reporting and billing purposes.

Cisco Equipment

To configure the various Cisco entities the following procedures are required.

CUCM

- 1 Configure the CUCM to send and receive calls from the H.323 network.
 - a With Neighbored IOS and CMA Gatekeepers
 - **b** With CMA Gatekeeper
 - c With IOS Gatekeeper

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

IOS Gatekeeper

• Set up zones and gateway type prefixes to enable dialing to DMA and Collaboration Server systems.

IOS and CMA Gatekeepers (Neighbored)

• Configure the Cisco IOS Gatekeeper for two separate zones.

Polycom Equipment

The following table lists the Polycom products supported within the various Deployment Architecture.

Only Collaboration Server configurations are described in detail in this document.

Configuration procedures for all other solution components are described in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Supported Polycom products

Polycom TIP and SIP	Version(s)
Polycom DMA 7000 system	V4.0
Polycom RealPresence Collaboration Server (RMX) 2000 and RealPresence Collaboration Server (RMX) 4000 systems	V7.6 and higher
Immersive Telepresence Systems: RPX 200 and 400 systems OTX 300 system TPX HD 306 system ATX HD 300 system	V3.0.3 Requires TIP option key. Requires Polycom Touch Control.
HDX Systems: 7000 HD Rev C 8000 HD Rev B 9006 4500	V3.0.3 Requires TIP option key.

The following Polycom peripheral: Polycom Touch Control	1.3.0
SIP ONLY (no TIP support)	Version(s)
Spectralink wireless phones 8020/8030	
Polycom VVX 1500	V4.0
Polycom VVX 1500 C	V3.3.1
KIRK Wireless Server 300/600v3/6000	

The following procedures 1 -16 are a summary of the configuration procedures.

The detailed procedures **1** - **16** begin with Procedure 1: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag.

Configuring the Collaboration Server

- 1 Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag
- 2 Configuring the Collaboration Server to statically route outbound SIP calls to DMA or CUCM
- 3 Configuring the Collaboration Server's H.323 Network Service to register with CMA gatekeeper
- 4 Configuring a TIP enabled Profile on the Collaboration Server
- 5 Configuring an Ad Hoc Entry Queue on the Collaboration Server if DMA is not used
- 6 Configuring a Meeting Room on the Collaboration Server
- 7 Configuring Participant Properties for dial out calls

Configuring DMA

If *DMA* is present in the configuration perform procedures **Configuring DMA to route SIP calls to CUCM** and **Configuring a Virtual Meeting Room (VMR)**, otherwise skip to procedure **Configuring CMA to route H.323 calls to Collaboration Server**.

- 8 Configuring DMA to route SIP calls to CUCM
- **9** Configuring a Virtual Meeting Room (VMR)

The procedures for configuring DMA are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Configuring CMA

- 10 Configuring CMA to route H.323 calls to Collaboration Server
- 11 Configuring CMA for use with Cisco IOS Gatekeeper (Neighbored)
- 12 Configuring CMA to route H.323 calls to CUCM
- 13 Configuring CMA to route non-H.323 calls to CUCM

The procedures for configuring CMA are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Configuring Endpoints

14 Configuring H.323 endpoints to register to the CMA or IOS gatekeeper

The procedures for configuring H.323 endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

15 Configuring SIP endpoints to register to:

- a DMA as SIP Proxy
- **b** CUCM as SIP Proxy

The procedures for configuring SIP endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

- 16 Configuring TIP endpoints to register to:
 - a DMA
 - **b** CUCM

The procedures for configuring TIP- enabled endpoints are described in detail in the *Polycom Unified Communications Deployment Guide for Cisco Environments*

Configuring Entry Queues and IVR Services

Conference IVR and Entry Queue/Virtual Entry Queues are supported with AVC TIP protocol in conferences that include both TIP-enabled and non-TIP-enabled endpoints.

A Virtual Entry Queue can be configured to either IVR Only Service Provider or External IVR Control mode.

TIP-enabled endpoints can be moved from the Entry Queue to the destination conference if the TIP Compatibility Modes settings in the Profile are identical for both conferencing entities (it is recommended to use the same Profile for both entities).

TIP IVR users can access the conference directly or enter the Entry Queue/Virtual Entry Queue and provide a password to access the conference.

The IVR services can be enabled for all TIP Compatibility Modes:

- Video only
- Video and Content
- Prefer TIP

IVR media files, WAV for voice messages and JPG for video slides, are all stored on the Collaboration Server.

Guidelines

- IVR default audio files are enabled for all TIP Compatibility Modes.
- Only Polycom default Welcome slides are available. Custom Welcome slides are not supported.
- TIP-enabled endpoints can send DTMF digits to MCU.
- In an mixed TIP environment there is no support for content in cascaded conferences.

Entry Queue and Virtual Entry Queue Access

TIP endpoints can dial-in to conferences directly using the IVR, Entry Queue/Virtual Entry Queue and IVR Only Service Provider.

Configuring the Conference and Entry Queue IVR Services

The IVR module includes two types of services:

- Conference IVR Service that is used with conferences
- Entry Queue IVR Service that is used with Entry Queues

The configuration process is the same for TIP and non-TIP enabled Conferences and Entry Queues.

Content

Polycom and Cisco endpoints can share Content within a Cisco TelePresence environment. The content sharing experience depends on whether the endpoints are registered with the DMA or CUCM.

Endpoint Registration Options - Content Sharing Experience

Multipoint Calls on Collaboration Server	Content Sharing	People + Content
Endpoints Registered to DMA		
HDX/ITP to HDX/ITP	Yes	Yes
HDX/ITP to Cisco CTS	Yes	Yes
Cisco CTS to HDX/ITP	Yes	No
Endpoints Registered to CUCM		
HDX/ITP to HDX/ITP	Yes	No
HDX/ITP to Cisco CTS	Yes	No
Cisco CTS to HDX/ITP	No	No

H.239

- ➤ A variety of resolutions and frame rates are supported. For more information see H.239 / People+Content.
- Can be used with SIP and H.323 endpoints, desktop (CMAD), room systems (HDX) and ITP (OTX, RPX).
- Not supported by Lync clients, IBM clients and Cisco CTS endpoints.
- > Cannot be used when HDX endpoints are registered to CUCM.
- TIP
 - > The resolution is fixed at XGA at 5fps.
 - Supported on HDX, Polycom ITP and Cisco CTS systems.
- The following content compatibility options are available:
 - ➤ Tip not enabled CTS cannot join the conference, all other endpoints can share H.239 content.

- TIP video compatibility CTS receives people video, all other endpoints can share H.239 content.
- ➤ TIP video and content compatibility CTS and HDX can share TIP content, all other endpoints receive only the people video.

For more information see Procedure 4: Configuring a TIP Enabled Profile on the Collaboration Server.

Procedure 1: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag

The **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag determines the minimum line rate at which an Entry Queue or Meeting Room can be TIP enabled.

CTS version 7 requires a minimum line rate of 1024 kbps and will reject calls at lower line rates, therefore the SysCollaboration Servertem Flag value must be 1024 or higher.

HD Video Resolutions for TIP calls are determined according to the following table:

TIP HD Video Resolution by Line Rate

Line Rate	Video Resolution
Line Rate >=3Mbps	HD1080p30
3Mbps > Line Rate >= 936kbps	HD720p30
Line Rate < 936kbps	Call is dropped.

For more information see Modifying System Flags.

Procedure 2: Configuring Collaboration Server to statically route outbound SIP calls to DMA or CUCM

- 1 In the IP Network Services Properties dialog box, click the SIP Servers tab.
- 2 In the SIP Server field, select Specify.
- 3 In the SIP Server Type field, select **Generic**.
- 4 Set Refresh Registration every 3600 seconds.
- 5 If not selected by default, change the Transport Type to TCP.
- 6 In the SIP Servers table:
 - **a** Enter the IP address of the DMA or CUCM in both the Server IP Address or Name and Server Domain Name fields.
 - **b** The Port field must be set to it's default value: **5060**. DMA and CUCM use this port number by default.
- 7 In the Outbound Proxy Servers table:
 - **a** Enter the IP address in the Server IP Address or Name field. (The same value as entered in Step 6a.)

🦐 Networking » IF Network Service Name: IF Network Service Routers 11.323 8 SIP >> Conferencing Gatekseper Specify Forts SIP Server Type: Generic > 05S SIPServers Security SIP Advenced y VBS (Sateway) 3600 seconds Refresh Registration every: Transport Type: TCP ▼ Create Certificate ▼ Send Certificate Certificate Method: SIP Servers: Paramete Frimary Server Alternate Server Server T 10.226.24.10 Server 10.226.24.10 5060 Outbound Proxy Servers: Paramete Primary Serve Server I 10,226,24,10 5060 CK Cancel

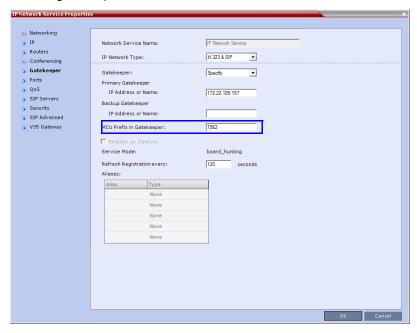
b The Port field must be set to it's default value: 5060.
(By default, the Outbound Proxy Server is the same as the SIP Server.)

When configuring Collaboration Server to statically route SIP calls to DMA or CUCM, it is important to also configure the Collaboration Server's H.323 Network Service to register with CMA gatekeeper. For more information see Procedure 3: Configuring the Collaboration Server's H.323 Network Service to register with CMA gatekeeper.

Procedure 3: Configuring the Collaboration Server's H.323 Network Service to register with CMA gatekeeper

1 In the IP Network Services Properties dialog box, click the **Gatekeeper** tab.

2 In the MCU Prefix in Gatekeeper field, enter the prefix that the Collaboration Server uses to register with the gatekeeper.

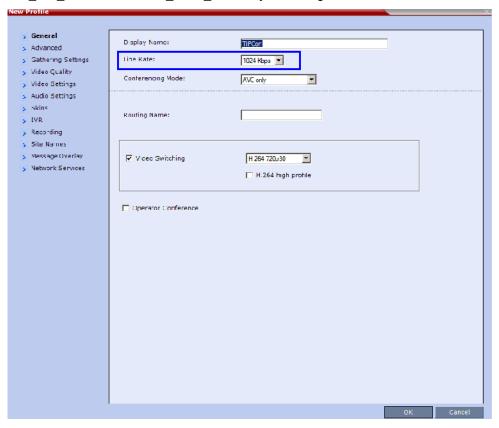


Procedure 4: Configuring a TIP Enabled Profile on the Collaboration Server

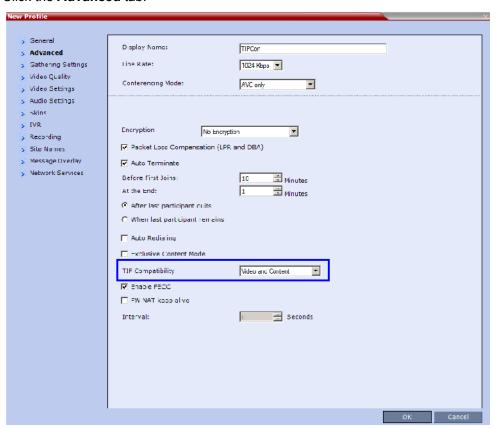
TIP enabled profiles must be used for the Entry Queues and Meeting Rooms defined on the Collaboration Server. (Different Profiles can be assigned to Entry Queues and Meeting Rooms, however they must be TIP enabled.) When TIP is enabled in the Profile, Gathering Settings and Message Overlay options are disabled.

1 Create a New Profile for the Meeting Room.

2 In the New Profile - General tab, set the Line Rate to a value of at least that specified for the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag in Procedure 1.

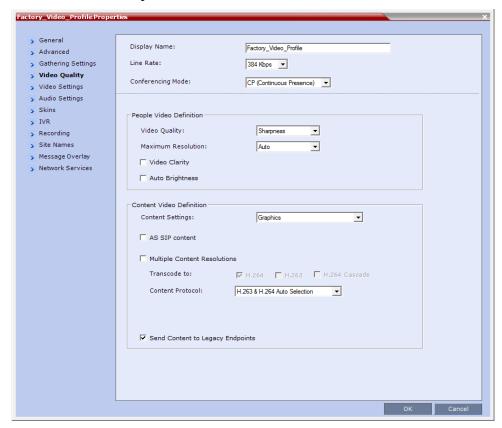


3 Click the Advanced tab.



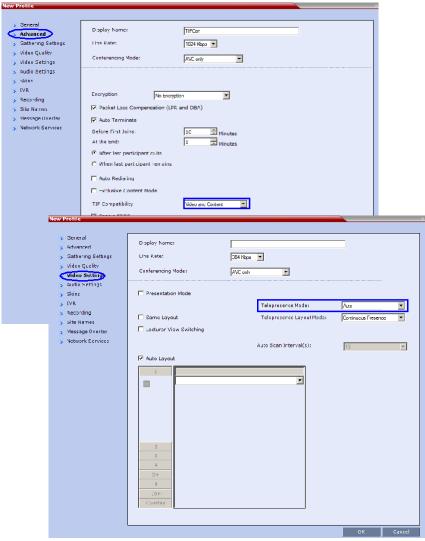
4 Select the TIP Compatibility mode according to the Content Sharing Behaviortables that are listed at the end of this procedure: Video and Content is recommended.

5 Click the Video Quality tab.



Content Settings is disabled if TIP Compatibility is set to Video and Content in the Advanced tab.

6 Click the Video Settings tab.



- 7 Set the Telepresence Mode to Auto.
- 8 Assign the New Profile to the Meeting Room. For more information see Creating a New Meeting Room.

Content Sharing Behavior

The following tables list the system's Content sharing behavior for the various combinations of TIP Compatibility mode settings and the following endpoints:

Polycom Immersive Telepresence Systems (ITP) Version 3.0.3:

- > RPX 200
- > RPX 400
- ➤ OTX 300
- > TPX HD 306
- > ATX HD 300

Polycom video conferencing endpoints (HDX) Version 3.0.3:

- > 7000 HD Rev C
- > 8000 HD Rev B
- > 9006
- **>** 4500

Cisco TelePresence® System (CTS) Versions 1.7 / 1.8:

- > CTS 1000
- > CTS 3000

TIP Compatibility - None

None		Content Receiver		
		HDX / ITP	CTS	
Content Sender	HDX / ITP	Media: H.264 Flow Control: H.323 via H.239 SIP via BFCP	Not Connected	
CTS		Not Connected	Not Connected	

TIP Compatibility - Video Only

Video Only		Content Receiver		
		HDX / ITP		стѕ
Content Sender	HDX / ITP		H.264 H.323 via H.239 SIP via BFCP	None
CTS		None		None

TIP Compatibility - Video & Content

Video & Content		Content Receiver		
		HDX / ITP		стѕ
Content	HDX* / ITP		H.264 H.323 via H.239	
Sender CTS			SIP via BFCP TIP via Auto Collaborati	on

^{*} If HDX supports TIP Content.

Selecting TIP Compatibility as Video and Content disables Content Settings in the Video Quality tab.

TIP Compatibility - Prefer TIP

Prefer TIP		Content Receiver		
		HDX / ITP		стѕ
Content	HDX / ITP	Media: Flow Control:	H.323 via H.239	
Sender CTS*			SIP via BFCP TIP via Auto Collaborati	ion

^{*} CTS Version 1.9.1 and higher support H.264 Content.

In **Prefer TIP** mode, it is pre-requisite that the *CTS* and *CUCM* versions support *H.264* base profile content without restrictions and that the *CTS* version be 1.9.1 or higher and that *CUCM* version be version 9.0 or higher.

Procedure 5: Configuring an Ad Hoc Entry Queue on the Collaboration Server if DMA is not used

1 Create or select the **Entry Queue** as described in **Entry Queues**.



2 In the New Entry Queue or Entry Queue Properties dialog box, ensure that Ad Hoc is selected.

3 Ensure that the Entry Queue is designated as the **Transit Entry Queue** as described in Setting a Transit Entry Queue.



Procedure 6: Configuring a Meeting Room on the Collaboration Server

The Profile for the Meeting Room must be TIP enabled as described in Procedure 4.

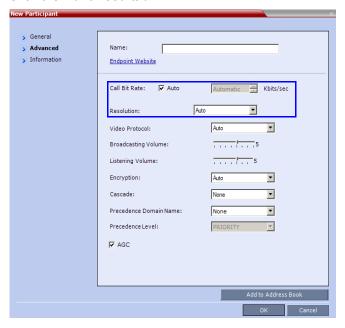
For more information see Creating a New Meeting Room.

Procedure 7: Configuring Participant Properties for dial out calls

Participant Properties must be configured to ensure that defined participants inherit their TIP settings from the Profile assigned to the Meeting Room.

a Define the New Participant's General settings. For more information see Adding a Participant to the Address Book.

b Click the **Advanced** tab.



- c Ensure that:
 - ♦ Call Bit Rate is set to Automatic or at least equal to or greater than the value specified by the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag.
 - ♦ Resolution is set to Auto or at least HD 720.
 - Video Protocol is set to Auto or at least H.264.

Collaboration with Microsoft and Cisco

This solution enables Polycom, Microsoft and Cisco users, each within their own environment, to participate in the same conference running on an Collaboration Server.

The Collaboration Server natively inter-operates with Microsoft Lync and Cisco TelePresence Systems, ensuring optimum quality multi-screen, multipoint calls between:

- Polycom Immersive Telepresence Systems (ITP) Version 3.1.1:
 - ➤ RPX 200
 - > RPX 400
 - ➤ OTX 300
- Polycom video conferencing endpoints
 - > Standalone HDX
 - > Polycom Group Series 300/500
- Microsoft
 - MS Lync (using MS-ICE)
 - > RTV 720p
- Cisco TelePresence® System (CTS) Versions 1.10

- > CTS 1300
- > CTS 3010

The deployment architecture in Single company with Polycom and Cisco Infrastructure - Polycom endpoints using SIP shows a company that has a mixture of Polycom, Cisco and Microsoft endpoints, room systems and telephony equipment that needs to enable multipoint calls between all its video and audio endpoints using the Collaboration Server as the conference bridge.

This solution enables Polycom, Microsoft and Cisco users, each within their own environment, to participate in the same conference running on an MCU.

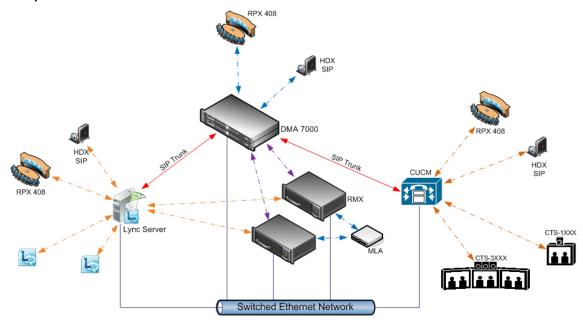
In the solution described in Single company with Polycom and Cisco Infrastructure - Polycom endpoints using SIP:

- DMA is required as all calls are dial-in to Virtual Meeting Rooms (VMR) provisioned on the DMA.
- Microsoft and Cisco clients dial the same VMR number to connect to the conference.
- Dial- out calls directly from the RMX are not supported.
- · Lync Clients cannot share content with CTS
- SIP trunks are required to the DMA from:
 - MS Lync as a Static Route.
 - > CUCM

Deployment Architecture

- DMA is required as all calls are dial-in to Virtual Meeting Rooms (VMR) provisioned on the DMA.
- Microsoft and Cisco clients dial the same VMR number to connect to the conference.
- Dial- out calls are not supported
- Lync Clients can not share content with CTS
- SIP trunks are required to the DMA from:
 - > MS Lync as a Static Route.
 - > CUCM

POCN Polycom, Microsoft and Cisco Infrastructure. Solution Architecture components.



.POCN Polycom, Microsoft and Cisco Infrastructure. Solution Architecture components

Component	Version
Polycom	
HDX	3.0.5
RSS	8.0
DMA	5.0
CMA	6.0.1
CMAD	5.2.3
ITP (OTX, RPX, ATX, TPX)	225
Conferencing for Outlook (PCO)	1.0.7
Touch Control	1.3
Microsoft	
Microsoft Lync 2010 Server	4.0.7577.223(CU10)
Microsoft Lync 2013 Server	5.0.8308.556 (CU3)
Microsoft Lync 2010 client	4.0.7577.4051 CU4
Exchange 2007 R2 SP3	8.3.213.1

Component	Version
Exchange 2010 SP2	14.2.247.5
Outlook 2007	12.0.6557.5001 SP2
Outlook 2010	14.0.6112.5000
Cisco	
CUCM	8.5, 8.6.2
Cisco Unified Personal communicator	8.5(2),8.5(5)
Cisco Unified IP Phones 7960, 7961, 7962, 7965, 7975	CUCM 8.5 / CUCM 8.6(2) Compatible
CTS	1.7.4, 1.8.1
C90, C20	TC5.0

The following are not supported:

- In the Lync environment:
 - > Sending or receiving Content.
 - > Dial-out to Lync clients.
 - > Presence of VMRs
- In the Cisco environment:
 - > TLS and SRTP
 - ➤ OBTP

Call Flow

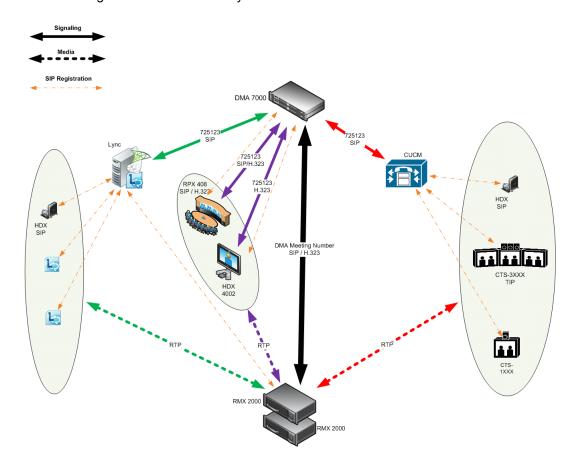
Multipoint Calls using DMA

In this example:

• Endpoint registration: To either DMA, Lync or CUCM.

• DMA dial in Prefix: 72

Virtual Meeting Room in DMA: 725123DMA Meeting Number: Generated by DMA



Administration

The various deployment combinations and settings within the Deployment Architecture affects the administration of the system.

DMA

The DMA system can be configured as a SIP proxy and registrar for the environment as well as a Gatekeeper for dial in H.323 calls. When configured as a Gateway for dial in H.323 calls, it enables H.323 endpoints to connect to the same VMR as SIP clients.

When used as a SIP peer, the DMA system can host video calls between Cisco endpoints that are registered with the CUCM, Lync Clients that are registered with the Lync Server and Polycom endpoints that are registered with the DMA system.

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*, *Using a Polycom DMA System as SIP Peer*.

Microsoft Lync Server

Microsoft Lync Server manages Presence for each registered Polycom endpoint and enables video calls between Lync Clients and Polycom endpoints allowing Lync contacts to be called without needing to know their addresses.

RTV video, MS-ICE and Lync-hosted conferencing are supported when Polycom endpoints are registered to Lync Server. Polycom endpoints use H.264, while Lync Clients use the RTV protocol.

CUCM

When Polycom SIP endpoints (voice and video) are registered directly with CUCM you can take advantage of supported telephone functions. CUCM may not support the full range of codecs and features available on the Polycom equipment. CUCM supported codecs and features will be used in such cases.

For more information see the Polycom Unified Communications Deployment Guide for Cisco Environments, Direct Registration of Polycom Endpoints with the Cisco Unified Communications Manager Participants.

Solution Interoperability Table

The following table lists components and versions of the Collaboration Server, Microsoft and Cisco Telepresence Systems (CTS) Integration Solution Architecture.

Solution Architecture Components

Component	Version	Description
CISCO Equipment		
CUCM	9.0.1	 Cisco Unified Communication Manager: CUCM must be configured to route calls to ASR/SBC. CUCM must be configured with a SIP trunk to the Service Provider's SBC. All endpoints must register once with the CUCM SIP trunks from CUCM to Polycom system components (eg. DMA) should be configured with Music on Hold disabled.

Component	Version	Description	
ASR (Cisco SBC)	100x	The Cisco Aggregation Services Routers (ASR) Series includes Cisco IOS XE Software Internetwork Operating System - Gatekeeper.	
		It controls and manages real-time multimedia traffic flows between IP/SIP network borders, handling signaling, data, voice, and video traffic.	
Polycom Equipmer	nt		
DMA	6.0.0_ATT_B uild_25	 Polycom Distributed Media Application DMA is an optional component but is essential if Content sharing is to be enabled. All SIP endpoints register to DMA as a SIP Proxy. DMA should be configured to route SIP calls (with CTS destination) to CUCM. DMA can be configured with a VMR (Virtual Meeting Room). Incoming calls are then routed to the Collaboration Server. 	
Collaboration Server	8.1.1	 MCU: Functions as the network bridge for multipoint calls between <i>H.323</i>, <i>SIP</i> and <i>TIP</i> endpoints. The Collaboration Server can be interfaced to <i>CUCM</i> using a <i>SIP</i> trunk, enabling <i>CTS</i> to join multipoint calls on Collaboration Server. Signaling goes through the <i>CUCM</i> while the media in <i>TIP</i> format goes directly between the <i>CTS</i> and Collaboration Server. The Collaboration Server must be configured to route outbound SIP calls to DMA. Collaboration Server must be configured to send and receive RTP streams to and from the Service Provider's SBC. 	
MLA Server	3.0.5	Multipoint Layout Application Required for managing multi-screen endpoint layouts for Cisco CTS 3XXX, Polycom TPX, RPX or OTX systems.	
HDX and ITP Endpoints	3.1.1.1	Telepresence, desktop and room systems. • Polycom SIP endpoints must register to DMA as SIP Proxy.	
Microsoft			
Lync 2010	4.0.7577.183 CU4		
Lync 2010 client	4.0.7577.405 1 CU4		
Exchange 2007 R2 SP3	8.3.213.1		
Exchange 2010 SP2	14.2.247.5		
Outlook 2007	12.0.6557.50 01 SP2		

Component	Version	Description
Outlook 2010	14.0.6112.50 00	

TIP Layout Support & Resource Usage

Cisco Telepresence endpoints using TIP protocol support only one (CTS 1000) or three (CTS 3000) display screens. Therefore, Polycom Telepresence endpoints will adjust their display to use one or three screens as follows:

- OTX system works with three screens, therefore no adjustment is required and it should be set to
 work in room switch Telepresence Layout Mode (while avoiding zooming in/out)
- RPX 2xx This endpoint works with two screens, therefore it will adjust to use only one screen.
- RPX 4xx This endpoint works with four screens, therefore it will adjust to use only three screens.
- Standalone HDX behaves as the CTS 1000 and uses only one screen.
- Group system 300/500 behaves as the CTS 1000 and uses only one screen.

The Polycom MLA Server manages the conference template layouts for Telepresence systems.

The number of screens used by each TIP-enabled endpoint is determined during the capabilities exchange phase of the dial-in connection. It affects the usage and allocation of resources used with TIP-enabled endpoints.

Supported TIP Resolutions and Resource Allocation

Supported Resolutions

In a Telepresence TIP-enabled environment, only two video resolutions are available: 720p30 & 1080p30.

Supported resolution per conference line rate

Conference Line Rate	Selected Resolution
3Mb or higher	1080p 30 fps
963kbps to 3Mb	720p 30 fps
Up to 936kbps	Call is disconnected.

Resource Allocation

The MCU media processor (ART) supports up to three TIP-enabled screens as follows:

- One TIP-enabled endpoint with three screens
- Up to three TIP-enabled endpoint with one screen

TIP-enabled endpoint with three screens must be handled by the same media processor. This endpoint may fail to connect if there is no one fully free media (ART) processor available.

The MCU will always try to fill up one media processor with up to three TIP-enabled endpoint with one screen, to save free media processors for TIP-enabled endpoint with three screens.

When monitoring an ongoing Telepresence conference with TIP-enabled endpoints (Cisco and Polycom), virtual participants are used to indicate the additional screens in the in the Web Client. For example, if the endpoint has three screens, the system will display three participants, one for each screen.

An additional virtual Audio Only participant is used for the audio only telephone connected to the TIP endpoint.

System capacity per MPMx card and resolution is summarized in the following table:

MPMx Resolution Capacities

No. of media processors (ART) per card	No. of TIP screens per media processor	720p30 ports	1080p30 ports
10	3	30	15

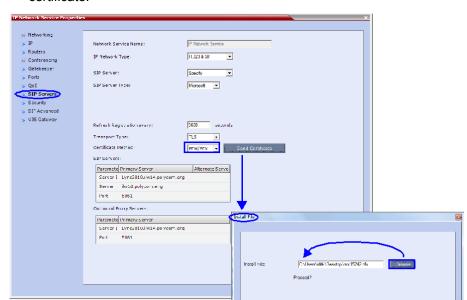
Configuring the Microsoft, Cisco and Polycom Components

1 Configure a SIP Trunk connection between the Polycom DMA system and the Cisco Unified Communications Manager (CUCM).

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*

- 2 Register the Collaboration Server to the Lync Server
 - Install a Security Certificate on the Collaboration Server.
 The Certificate is obtained from the System Administrator and saved on the Workstation.
 - **b** In the SIP Servers tab of the IP Network Services Properties dialog box:
 - i In the Certificate Method drop-down menu, select PEM/PFX.
 - ii Click the Send Certificate button.

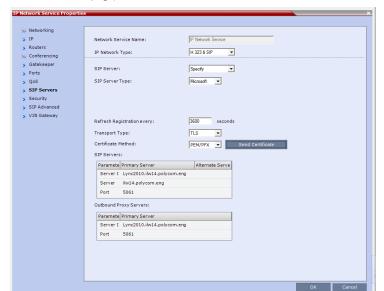
The Install File dialog box is displayed.



iii Browse to the saved Certificate on the Workstation and click the **Yes** button to install the certificate.

For more information see:

- ◆ Appendix H Integration Into Microsoft Environments.
- ♦ The Polycom Unified Communications Deployment Guide for Cisco Environments.
- **3** Register the Collaboration Server with the *Lync Server*.
 - a In the IP Network Services Properties dialog box, click the SIP Servers tab.
 - **b** In the SIP Server field, select **Specify**.
 - c In the SIP Server Type field, select Microsoft.
 - d Set Refresh Registration every 3600 seconds.
 - e If not selected by default, change the Transport Type to TLS.
 - f In the SIP Servers table, enter the IP address of the Lync Server in both the Server IP Address or Name and Server Domain Name fields.
 - g In the SIP Servers table, the Port field must be set to 5061.
 - **h** In the Outbound Proxy Servers table, enter the IP address in the Server IP Address or Name field. (The same value as entered in **Step f**.)



i In the Outbound Proxy Servers table, the Port field must be set to 5061. (The same value as entered in Step g.)

For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*

- 4 Set the ITP_CERTIFICATION System Flag to YES.
 When set to NO (default), this flag disables the Telepresence features in the Conference Profile.
- 5 Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag.
 - The **MIN_TIP_COMPATIBILITY_LINE_RATE** System Flag determines the minimum line rate at which a Profile can be TIP enabled.
 - CTS version 1.7 requires a minimum line rate of 1024 kbps and will reject calls at lower line rates, therefore the System Flag value must be **1024** or higher.
- 6 If required, manually add and set the FORCE_720P_2048_FOR_PLCM_TIP System Flag using one of the following values:
 - **FORCE_720P_2048_FOR_PLCM_TIP (Default)** Forces HD 720p video resolution and a line rate of 2048kbps for all Polycom TIP-enabled endpoints that connect to the TIP-enabled Telepresence conference. This setting is the recommended setting.
 - **FORCE_2048_FOR_PLCM_TIP** Forces a line rate of 2048kbps for all Polycom TIP-enabled endpoints connecting to the TIP-enabled Telepresence conference.
 - **NO_FORCE** No forcing is applied and Polycom TIP-enabled endpoints can connect to the TIP-enabled Telepresence conference at any line rate or resolution.
- 7 Reset the Collaboration Server.
- 8 For more information see .
- 9 Register the DMA to the Lync server
 - For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*
- 10 Register the ITP endpoints to the Lync server

11 Register Lync Clients to the Lync server.

For more information see the relevant Lync documentation.

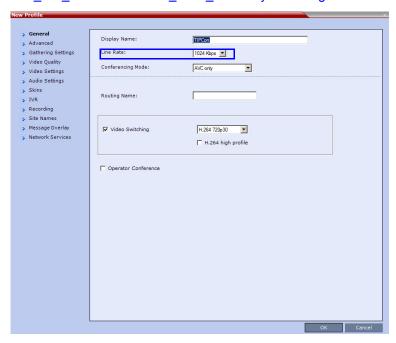
- 12 Register DMA to the CUCUM server
- **13** Register CTS1000 and CTS3000 endpoints to the CUCUM server For more information see the relevant Cisco documentation.
- **14** Register ITP endpoints to the CUCM server.
- 15 Register HDX endpoints to the DMA as Gatekeeper
- 16 Open MLA to configure ITP Layouts

MLA (Multipoint Layout Application) is required for managing CTS 3XXX layouts whether Polycom TPX, RPX or OTX systems are deployed or not. MLA is a Windows® application that allows conference administrators to configure and control video layouts for multipoint calls involving Polycom Immersive Telepresence (ITP) systems.

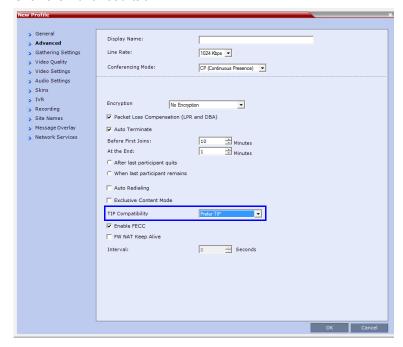
For more information see the *Polycom Unified Communications Deployment Guide for Cisco Environments*.

- **17** Configure a TIP Enabled Profile on the Collaboration Server.
 - a Create a New Profile for the Meeting Room.

b In the New Profile - General tab, set the Line Rate to a value of at least that specified for the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag in Procedure 1: Set the MIN_TIP_COMPATIBILITY_LINE_RATE System Flag.



c Click the Advanced tab.



d Select the **TIP Compatibility** mode according to the Content Sharing Behavior tables that are listed below.

Prefer TIP is recommended if *Polycom* endpoints are to connect using *TIP*, otherwise select **Video and Content**.



When Prefer TIP is selected Video Switching, Gathering Settings, Skins, Message Overlay, Site Names and Network Indication(s) are disabled.

Content Sharing Behavior

The following tables list the system's Content sharing behavior for the various combinations of TIP Compatibility mode settings and the following endpoints:

Polycom Immersive Telepresence Systems (ITP) Version 3.0.3:

- > RPX 200
- > RPX 400
- ➤ OTX 300
- > TPX HD 306
- > ATX HD 300

Polycom video conferencing endpoints (HDX) Version 3.0.3:

- > 7000 HD Rev C
- > 8000 HD Rev B
- > 9006
- **>** 4500

Cisco TelePresence® System (CTS) Versions 1.7 / 1.8:

- > CTS 1000
- > CTS 3000

TIP Compatibility - None

None		Content Receiver		
		HDX / ITP	стѕ	
Content Sender	HDX / ITP	Media: H.264 Flow Control: H.323 via H.239 SIP via BFCP	Not Connected	
	CTS	Not Connected	Not Connected	

TIP Compatibility - Video Only

Video Only		Content Receiver		
		HDX / ITP		стѕ
Content Sender	HDX / ITP	Media: Flow Control:	H.264 H.323 via H.239 SIP via BFCP	None
	CTS	No	one	None

TIP Compatibility - Video & Content

Video & Content		Content Receiver		
		HDX / ITP		CTS
Content HDX* / ITP	HDX* / ITP		H.264 H.323 via H.239	
Sender	CTS		SIP via BFCP TIP via Auto Collaborati	on

^{*} If HDX supports TIP Content.

Selecting TIP Compatibility as Video and Content disables Content Settings in the Video Quality tab.

TIP Compatibility - Prefer TIP

Prefer TIP		Content Receiver		
		HDX / ITP		стѕ
Content	HDX / ITP		H.264 H.323 via H.239	
Sender	CTS*		SIP via BFCP TIP via Auto Collaborati	on

^{*} CTS Version 1.9.1 and higher support H.264 Content.

In **Prefer TIP** mode, it is pre-requisite that the *CTS* and *CUCM* versions support *H.264* base profile content without restrictions and that the *CTS* version be 1.9.1 or higher and that *CUCM* version be version 9.0 or higher.

Encryption

Encryption between the RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 and a CISCO environment is supported. Media is encrypted using SRTP, while control is encrypted using SRTCP. TIP is encrypted using SRTCP. SIP is be encrypted using TLS. When upgrading, the Collaboration Server automatically creates a self-signed certificate to support encrypted communications with CISCO endpoints.

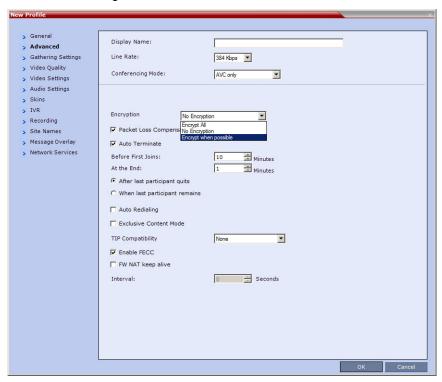
For media encryption. the Collaboration Server will first attempt to exchange keys using DTLS. If the Collaboration Server fails to exchange keys using DTLS, SIP TLS encrypted with SDES is used to exchange media encryption keys.

Guidelines

- This feature is not supported in Ultra Secure Mode.
- Voice activity metrics and RTP are not encrypted.
- In the event that DTLS negotiation fails, SIP will be encrypted using TLS if enabled in the IP Management Network properties, SIP Servers tab. DTLS negotiation does not require SIP TLS.
 - ➤ In a mixed CISCO and Microsoft Lync environment, in order to assure encrypted communications with both CISCO endpoints and Microsoft Lync in the event of DTLS negotiation failure, the certificate defined in the IP Management Network Services properties dialog box, SIP Servers tab, must have been issued by the same certificate authority that issued the certificates used by both the Microsoft Lync server and the CUCM server.
- The flag, SIP_ENCRYPTION_KEY_EXCHANGE_MODE, is used to control this feature. The
 possible values are:
 - > AUTO (default): Normal encryption flow
 - > DTLS: Only use DTLS for encryption
 - > SDES: Only use SDES (SRTP) for encryption
 - NONE: Encryption is disabled
- The feature was tested using the following CISCO components:
 - Cisco CUCM Version 9.0
 - Cisco TPC Version 2.3
 - Cisco endpoints running Version 1.9.1
 - ♦ C20, C40, C60, and C90 running TC5
 - ♦ CTS500
 - ♦ CTS1310
 - ♦ CTS3010

To enable DTLS negotiation for content encryption:

1 In a new or existing Profile, click the Advanced tab.

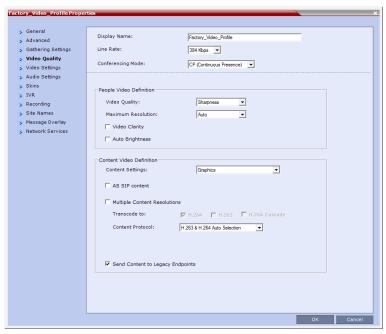


- 2 Set Encryption to either Encrypt All or Encrypt when possible.
- 3 Set the FORCE_ENCRYPTION_FOR_UNDEFINED_PARTICIPANT_IN_WHEN_ AVAILABLE_MODE System Flag to NO

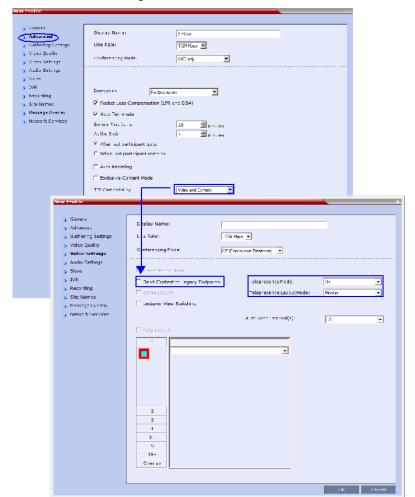
These setting will enable encrypted and non-encrypted *H.323* participants to connect to encrypted or non-encrypted conferences.

For more information see Encryption.

a Click the Video Quality tab.



Content Settings is disabled if TIP Compatibility is set to Video and Content in the Advanced tab.



b Click the *Video Settings* tab.

- **c** Set the *Telepresence Mode* to **Auto/On** and select the *Telepresence Layout Mode*.
- **4** Assign the *New Profile* to the *Meeting Room*. For more information see Creating a New Meeting Room.
- 5 Configure a Virtual Meeting Room (VMR) on the DMA.
 The procedures for configuring DMA are described in detail in the Polycom Unified Communications Deployment Guide for Cisco Environments.

Resolution Configuration

The resolution configuration dialog box is not applicable to TIP-enabled conferences as it uses fixed settings:

HD Video Resolutions for TIP calls are determined according to the following table:

TIP HD Video Resolution by Line Rate

Line Rate	Video Resolution
Line Rate >=3Mbps	HD1080p30
3Mbps > Line Rate >= 936kbps	HD720p30
Line Rate < 936kbps	Call is dropped.

Endpoints

- 1 Configure HDX endpoints to register to Lync Server.
- 2 Configure H.323 endpoints to register to DMA as SIP Proxy
- **3** Configure *SIP* endpoints to register to:
 - ♦ DMA as SIP Proxy
 - ♦ Lync Server as SIP Proxy
 - ♦ CUCM as SIP Proxy
- **4** Configure *TIP* endpoints to register to:
 - ◆ DMA
 - ♦ CUCM

For more information on the above, see *Polycom Unified Communications Deployment Guide for Cisco Environments*.

Content

Endpoint Registration and Dialing Method affect the Video and Content Sharing characteristics of the conference as detailed in Table 5-9.

Video and Content

	Endpoint Registration			
	Lync	CUCM	DMA	
Dialing Method	ITP /HDX RTV Key is required for HDX and ITP	ITP /HDX TIP Key is required for HDX	ITP /HDX TIP Key is required for HDX	
HDX to Collaboration Server	HD H.264 VideoSIP P+CContent: XGA,5fpsICE	HD H.264 VideoNo ContentICE not supported	HD H.264 VideoSIP P+CContent: XGA,5fpsICE not supported	
Lync to Collaboration Server	HD Video (RTV)No Content SharingContent sent to Lync to	using Content for Legacy En	ndpoints	

	Endpoint Registration			
	Lync	CUCM	DMA	
Dialing Method	ITP /HDX RTV Key is required for HDX and ITP	ITP /HDX TIP Key is required for HDX	ITP /HDX TIP Key is required for HDX	
CTS to Collaboration Server	HD1080p30TIP Content SharingContent: XGA,5fps			

Operations During Ongoing Conferences

Moving participants between TIP enabled meetings and non TIP enabled meetings is not possible.

Monitoring

CTS Participants

1 In the *Participant List* pane double-click the participant entry. Alternatively, right-click a participant and then click **Participant Properties**.

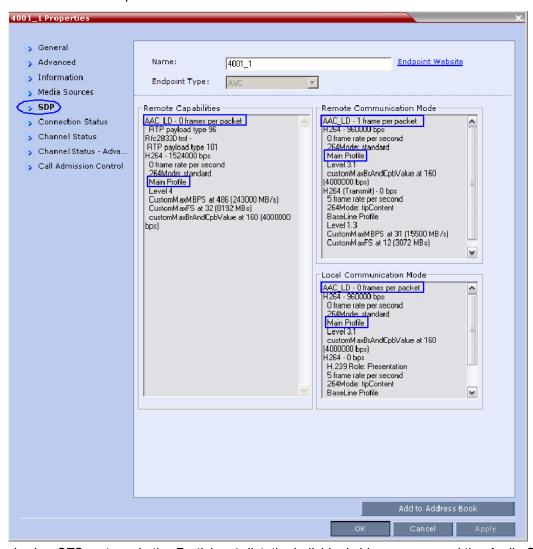
The Participant Properties - General dialog box opens.

2 Click the SDP tab.

The following are indicated in the *Remote Capabilities*, *Remote Communication Mode* and *Local Communication Mode* panes:

> AAC_LD - Audio Protocol

Main Profile - Video protocol



When viewing CTS systems in the Participants list, the individual video screens and the Audio Channel (AUX) of the CTS system are listed as separate participants. The Participant list below shows a connected CTS 3000, a 3-screen system.



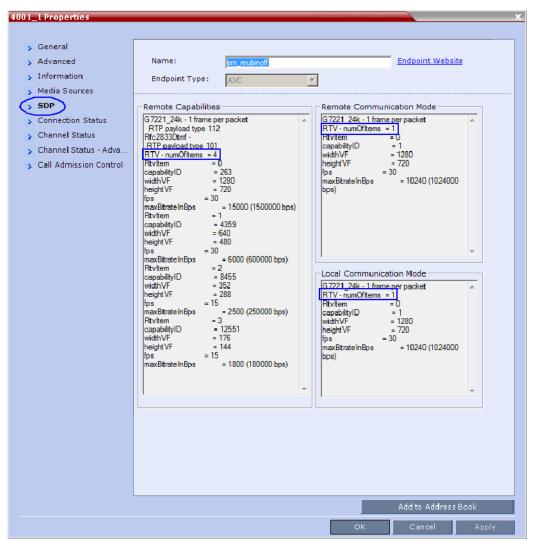
Lync Participants (RTV)

1 In the *Participant List* pane double-click the participant entry. Alternatively, right-click a participant and then click **Participant Properties**.

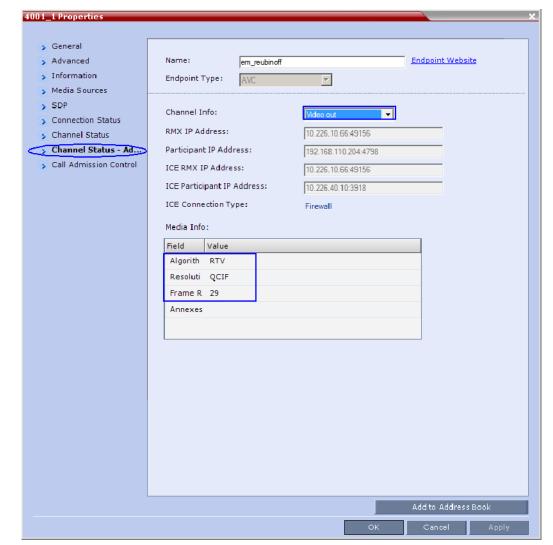
The Participant Properties - General dialog box opens.

2 Click the SDP tab.

RTV is indicated in the *Remote Capabilities*, *Remote Communication Mode* and *Local Communication Mode* panes:



- 3 Click the Channel Status Advanced tab
- 4 In the Channel Info drop-down menu select Video Out.



Media Info displays RTV Channel Status parameters:

Known Limitations

The following may occur in the collaborative environment:

- Artifacts and ghosting may appear when Lync Clients and CTS endpoints connect to the VMR.
 Frequency: Seldom.
- Lync Client receives fast updates (Intra) from CTS 500 endpoints causing the screen to refresh repeatedly.

Frequency: Often.

- Audio volume and video quality decreases on CTS endpoints.
 Frequency: Seldom.
- *CTS* endpoint connects and then disconnects after a few seconds. Frequency: Seldom.
- Lync Clients always connect encrypted to non-encrypted conferences.

- Auto Layout sometimes ignored for CTS and Lync Clients calling through DMA.
 Frequency: Rarely.
- Content sent from HDX endpoint is received by all endpoints for 1 second before stopping.
 Conference is Content to Legacy enabled and TIP Compatibility is Video Only.
 Frequency: Often.

Appendix J - Restoring Defaults

You can erase the current Collaboration Server configuration and restore default factory settings. There are two Restore levels:

- Standard Restore
- Comprehensive Restore

This tool is intended for Administrator users, to be performed prior to RMA.

Standard Restore

The Standard Restore level (default setting) deletes the following files:

- CDR
- Address Book
- Log Files
- Faults
- Dump Files
- Notes

In addition all the conferencing entities are deleted:

- Entry Queues
- Profiles
- Meeting Rooms
- IVR Services
- Default Network IP Service

When the system is restarted, these conferencing entities are created based on the factory defaults. In addition, the *Fast Configuration Wizard* automatically opens, letting the user to define the Default IP Network Service.

Comprehensive Restore

In addition to the Standard Restore, the system deletes the:

- CFS license information
- Management Network Service

The MCU is restored to the settings it had when shipped from the factory. The *Product Activation Key* is required to re-configure the *Management Network Service* during the *First Entry Configuration*.

For more information see the *Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide, Chapter 2 Procedure 2: Product Registration .*

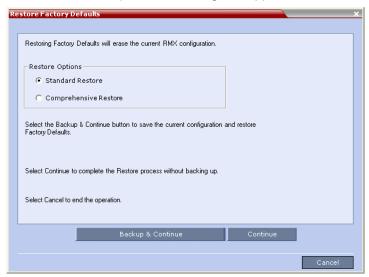
Restoring Factory Defaults

Restoring the Collaboration Server to Factory Defaults can be performed using the:

- Administration Tools in the Collaboration Server menu
 This method is used when the user can login with Administrator or Support system permissions.
- USB key
 This method is used when the user cannot login with Administrator or Support system permissions.

To Restore Factory Default Settings using Administration Tools in the Collaboration Server menu:

1 In the Collaboration Server menu, click Administration > Tools > Restore Factory Defaults.
The Restore Factory Defaults dialog box appears.



2 Select Standard Restore or Comprehensive Restore.



If the current conferencing entities and system configuration are to be restored after restoring the initial system settings it is recommended to use the *Backup & Continue* option.

- **3** Click one of the following buttons:
 - ➤ Backup & Continue Backup of the current Collaboration Server configuration. Proceed with step 4.
 - Continue Initializes all the current system configuration files and conferencing entities and then restores them to their factory values according to the selected restore level. Proceed with step 5.
 - Cancel Cancels and exits this dialog box.

4 Click the Backup & Configuration option.

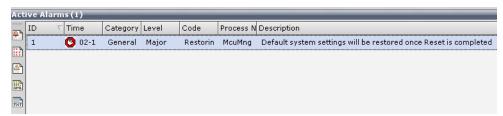
The Backup Configuration Dialog box opens.



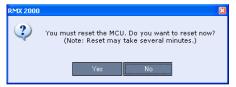
- **a** Click **Browse** to select the *Backup Directory Path* and select **Backup**. The system initiates the backup of Collaboration Server configuration files.
- **b** Optional. To exit click **Close**.
- **5** When the **backup** completes, a confirmation dialog box is displayed.



6 Click **Yes** to restore the Collaboration Server. An *Active Alarm* is activated.



7 Click **Yes**, to reset the Collaboration Server.



- **8** Login to the Collaboration Server using the *Web Client*, if you selected:
 - ➤ Standard Restore, the Fast Configuration Wizard appears. For more information, see the Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide, Procedure 4: Modifying the Default IP Service and ISDN/PSTN Network Service Settings.
 - ➤ Comprehensive Restore, requires initializing the First Entry Configuration procedures, as defined in the Polycom RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Getting Started Guide, Procedure 1: First-time Power-up.

USB Restore



Do **not** insert a *USB* device into the *Collaboration Server's USB* port unless it is your intention to disable *Secured Mode* or perform a *Comprehensive Restore to Factory Defaults*.

Restoring the Collaboration Server Using the USB Port can be used to set the Collaboration Server back to its factory default settings, if for any combination of factors the system becomes unstable or unmanageable.

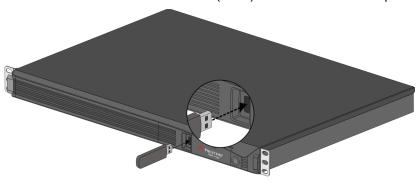
There are also administrative operations that cannot be performed on a *secured* or *ultra secured* system that require the Collaboration Server to be set back to its default (normal) security mode.



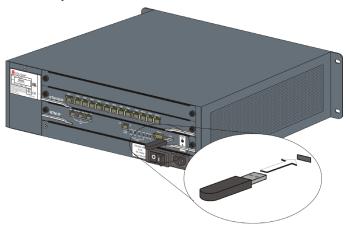
Do **not** use any *USB* ports other than the ones indicated in the following diagrams.

When performing operations using a USB device, the following USB ports are used:

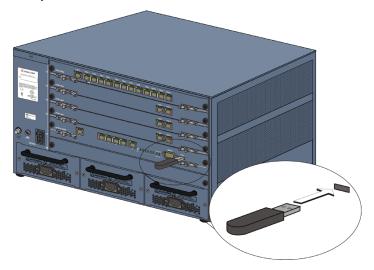
RealPresence Collaboration Server (RMX) 1500 - left most USB port on the front panel.



 RealPresence Collaboration Server (RMX) 2000 - at the bottom right corner of the RTM IP card on the back panel.



RealPresence Collaboration Server (RMX) 4000 - at the bottom right corner of the RTM IP 4000 card
on the back panel.



Recovery Operations Performed Using a USB Device

The USB port of a RealPresence Collaboration Server in Ultra Secure Mode can be used to:

- Perform a Comprehensive Restore to Factory Defaults
- Perform an Emergency CRL (Certificate Revocation List) Update

Recovery Options

The RMX has two recovery options:

- Comprehensive Restore to Factory Defaults
 Inserting a USB key with the following two text files will restore the RMX to factory defaults:
 - RestoreToFactoryDefault.txt
 - lan.cfg



Do **not** insert a *USB* key containing a file named *RestoreToFactoryDefault.txt* if the *USB* key does not also contain a *lan.cfg* file.

- Emergency CRL (Certificate Revocation List) Update
 Inserting a USB key or USB mouse and restarting the Collaboration Server will:
 - > Change the Collaboration Server from HTTPS mode to HTTP mode.
 - ➤ Disable *PKI Client Validation* so that the *Collaboration Servers* configuration or *CRLs* (or both) can be updated.

Comprehensive Restore to Factory Defaults

Inserting a USB key containing a file named RestoreToFactoryDefault.txt and a lan.cfg file will cause the Collaboration Server to exit Secure Mode and perform a Comprehensive Restore to Factory Defaults.

The Comprehensive Restore to Factory Defaults deletes the following files:

- CDR
- Address Book
- Log Files
- Faults
- Dump Files
- Notes

In addition all the conferencing entities are deleted:

- Entry Queues
- Profiles
- Meeting Rooms
- IVR Services
- Default Network IP Service
- Log Files
- · CFS license information
- Management Network Service

The Collaboration Server is restored to the settings it had when shipped from the factory. The *Product Activation Key* is required to re-configure the *Management Network Service* during the *First Entry Configuration*.

Performing a Comprehensive Restore to Factory Defaults

To perform a Comprehensive Restore to Factory Defaults:

Restoring the Collaboration Server to Factory Defaults consists of the following steps:

- Step 1: Backup Configuration Files. These files will be used to restore the system in Step 10.
- Step 2: Configure a workstation for Direct Connection.
- **Step 3:** Connect to the *Collaboration Server* and the workstation using a *LAN* cable.
- **Step 4:** Into the Collaboration Server's *USB* port, insert a *USB* key containing a file named *RestoreToFactoryDefault.txt* and also containing a *lan.cfg* file.



Do **not** insert a *USB* key containing a file named *RestoreToFactoryDefault.txt* if the *USB* key does not also contain a *lan.cfg* file.

- Step 5: Restart the Collaboration Server.
- **Step 6**: If you are not using a RealPresence Collaboration Server (RMX) 4000 continue with Step 9.

- **Step 7**: Into the Collaboration Server's *USB* port, insert a *USB* key containing a file named *lan.cfg* file only.
- Step 8: Restart the Collaboration Server.
- **Step 9:** From the workstation, connect to the *Collaboration Server's Alternate Management Network*.
- Step 10: Apply the Product Activation Key.
- Step 11: Unplug the USB key.
- Step 12: Restart the Collaboration Server.
- **Step 13:** Restore the *System Configuration* from the backup by applying the backup files created in procedure **Step 1**.
- Step 14: Restart the Collaboration Server.

(If the Collaboration Server is unresponsive after these procedures a further restart may be necessary.)

Step 1: Backup Configuration Files

The Software Management menu is used to backup and restore the RMX's configuration files and to download MCU software.

To backup configuration files:

a On the *Collaboration Server* menu, click **Administration > Software Management > Backup Configuration**.

The Backup Configuration dialog box opens.



b Browse to the Backup Directory Path and then click Backup.

Step 2: Configure a Workstation for Direct Connection

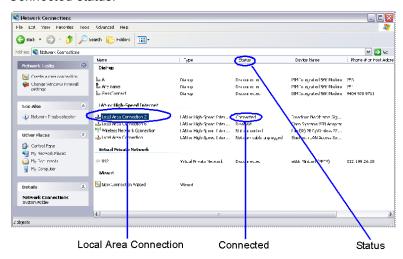
The following procedures show how to modify the workstation's networking parameters using the *Windows New Connection Wizard*.

For non-Windows operating systems an equivalent procedure must be performed by the system administrator.

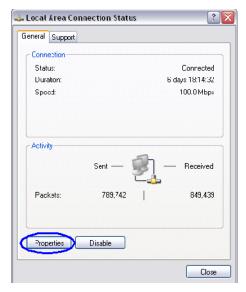
Before connecting directly, you must modify the *IP Address*, *Subnet Mask* and *Default Gateway* settings of the workstation to be compatible with the Collaboration Server's *Alternate Management Network*.

a On the Windows *Start* menu, select **Settings** > **Network Connections**.

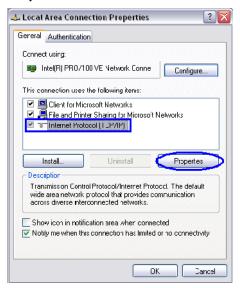
b In the *Network Connections* window, double-click the **Local Area Connection** that has *Connected* status.



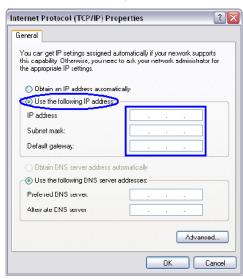
c In the Local Area Connection Status dialog box, click the Properties button.



d In the Local Area Connection Properties dialog box, select Internet Protocol [TCP/IP] > Properties.



- e In the Internet Protocol (TCP/IP) Properties dialog box, select Use the following IP address.
- f Enter the IP address, Subnet mask and Default gateway for the workstation.



The workstation's IP address should be in the same network neighborhood as the *RMX's Control Unit* IP address.

Example: IP address - near 169.254.192.nn



None of the reserved IP addresses listed in *Reserved IP Addresses* should be used for the *IP Address*.

The addresses needed for connection to the Collaboration Server's *Alternate Management Network* are listed in Table 5-10.

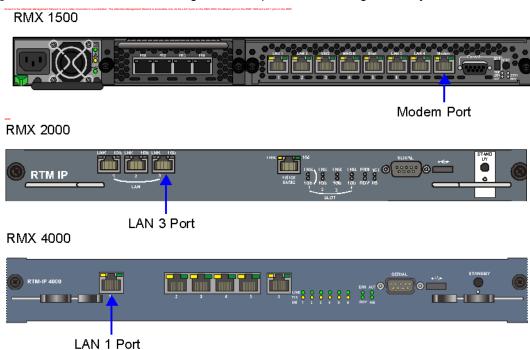
Reserved IP Addresses

Network Entity	Alternate Network IP Address
Control Unit IP Address	169.254.192.10
Control Unit Subnet Mask	255.255.240.0
Default Router IP Address	169.254.192.1
Shelf Management IP Address	169.254.192.16
Shelf Management Subnet Mask	255.255.240.0
Shelf Management Default Gateway	169.254.192.1

g Click the **OK** button.

Step 3: Connect the RMX to the Workstation

The Alternate Management Network enables direct access to the RMX for support purposes. The Alternate Management Network cannot be configured and operates according to factory defaults.



• Connect the cable between the *RMX* port and the LAN port configured on the workstation.

Step 4: Insert a USB key containing a file named RestoreToFactoryDefault.txt and a lan.cfg file into the USB port of the RMX

The *USB* port locations for RealPresence Collaboration Server (RMX) 1500/2000/4000 are shown in USB Restore .

Step 5: Power the RMX Off and then On.

- Step 6: If you are not using a RealPresence Collaboration Server (RMX) 4000 continue with Step 9.
- Step 7: Into the Collaboration Server USB port, insert a USB key containing a file named lan.cfg file only.
- Step 8: Restart the RMX.

Step 9: Connect to the Alternate Management Network

a Start the RMX Web Client application on the workstation, by entering http://169.254.192.10 (the Control Unit IP Address) in the browser's address line and pressing Enter.

The *Login* dialog box is displayed.



b In the Collaboration Server Web Client Login screen, enter the default Username (POLYCOM) and Password (POLYCOM) and click Login.

Step 10: Apply the Product Activation Key.

The *RMX Web Client* opens and the *Product Activation* dialog box appears with the serial number filled in.

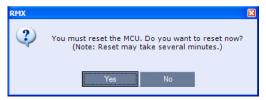


a In the Activation Key field, enter or paste the Product Activation Key obtained earlier.

b Click OK.

If you do not have an *Activation Key*, click **Polycom Resource Center** to access the *Service* & *Support* page of the Polycom website.

The system prompts with a restart dialog box:



Step 11: Unplug the USB device.

• Remove the *USB* device from the *USB* port of the Collaboration Server.

Step 12: Restart the RMX.

• In the restart dialog box, click Yes.

Step 13: Restore the System Configuration From the Backup.

To restore configuration files:

- a On the RMX menu, click Administration > Software Management > Restore Configuration.
- **b** Browse to the *Restore Directory Path* where the backed up configuration files are stored.
- c Click the Restore button.
- **d** When the **Restore** is complete, restart the *Collaboration Server* (**Step 14**). *RMX* system settings, *with the exception of User* data, are restored.
- **e** Restore *User* data by repeating **step** a to **step** d of this procedure.

Step 14: Restart the RMX.

Emergency CRL (Certificate Revocation List) Update

Administrators maintaining *RMX* systems are required to perform an update of the *CRLs* used on the systems within the validity period of the current *CRLs*.

Should the current *CRLs* expire; the system will not allow administrators to login and perform administrative tasks using the *RMX Web Client* or *RMX Manager*.

The *Emergency CRL Update* procedure disables client certificate validation enabling an administrator to access the system and install an updated *CRL* file without having to perform a full system rebuild.



This procedure must only be performed on a secured network as the system must disable the client certificate validation process resulting in management traffic being sent over the network without the use of *SSL* encryption.



The *RMX* must be powered on before starting this procedure.

To perform an Emergency CRL Update procedure:

- Step 1: Download and save the updated CRL files from the CA Server.
- Step 2: Disable Secured Communications Mode.
- Step 3: Open the Certification Repository.
- Step 4: Update the CRL files.
- Step 5: Update the Repository.
- **Step 6:** Re-connect to the *RMX*.
- Step 7: Re-enable Secured Communications Mode.

Step 1: Download and save the updated CRL files from the CA Server.

These files are saved on the workstation.



The RMX supports the use of PEM and DER formats.

Take note of the format you download as you will need to make a selection later in this process when uploading the new *CRL* files.

Step 2: Disable Secure Communications mode

- **a** Connect a *USB* keyboard or mouse to the *USB* port of *RMX*.
 - The USB port locations for RMX 1500/2000/4000 are shown in USB Restore.
- **b** Power the *RMX* **Off** and then **On** using the power switch and allow the *RMX* to complete its startup.

System restart can take 5 - 10 minutes, depending on the RMX's configuration.

Using the *RMX Manager*:

- **c** In the *MCUs* list, select the *RMX* to be updated.
- d In MCU Properties, change the Port number from 443 to 80.
- e Click OK.
- **f** In the *MCU*s list, select the *RMX* to be updated.
- **g** Right-click in the *MCUs* list entry and select **Connect**.
- h Click Accept to accept the warning banner.
- i Enter an administrator Username and Password.
- j Click OK.

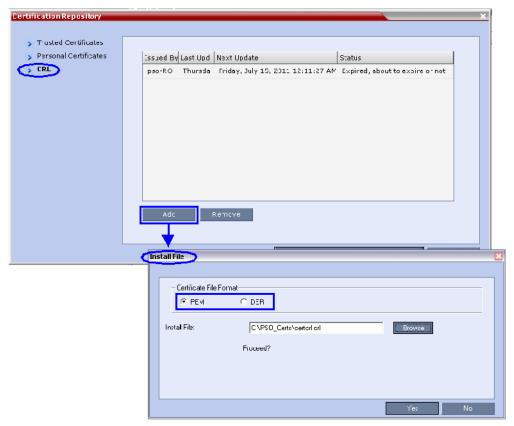
Step 3: Open the Certification Repository.

On the RMX menu, click Setup > RMX Secured Communication > Certification Repository.

Step 4: Update the CRL files.

In the Certification Repository:

- a Click the CRL tab.
- b Click Add.



- **c** In the *Install File* dialog box, select the **DER** or **PEM** format depending on which file format was chosen in *Step 1* of this procedure.
- **d** Click the **Browse** button to navigate to the folder on the workstation where you saved the *CRL* files in *Step 1* of this procedure.
- **e** Select the *CRL* file that you want to upload.
- f Click Yes to proceed.

The system checks the *CRL* file and displays a message that the certificate was loaded successfully.

g Repeat Steps *d* through *f* until all of the required *CRL* files has been updated.

Step 5: Update the repository.

When all the CRL files have been updated as Step 4: Update the CRL files. described in Step 4: Update the CRL files. Step 4:

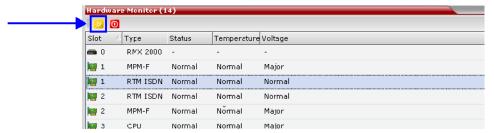
a Click Update Repository.

A repository update confirmation message is displayed.

b Click **OK** to update the repository.

Step 6: Re-connect to the RMX.

- a Remove the USB device that was connected in Step 2a.
- **b** Restart the *RMX*.
- **c** In the *RMX Management* pane, click the **Hardware Monitor** button. The *Hardware Monitor* pane is displayed.



d Click the **Reset** button.

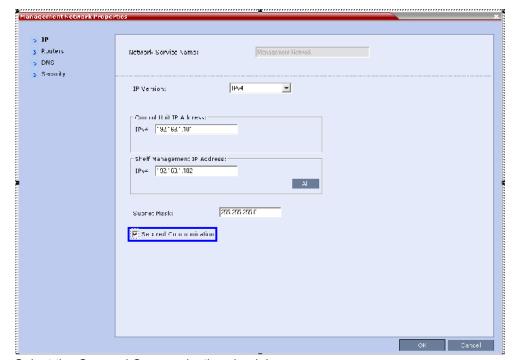
The *RMX* restarts. System restart can take 5 - 10 minutes, depending on the *RMX*'s configuration. Using the *RMX Manager*:

- **e** In the *MCU*s list, select the *RMX* to be updated.
- **f** Right-click in the *MCUs* list entry and select **Connect**.
- **g** Click **Accept** to accept the warning banner.
- **h** Enter an administrator *Username* and *Password*.
- i Click OK.

Step 7: Re-enable Secured Communications Mode.

Using the RMX Manager:

- a In the RMX Management pane, click the IP Network Services button. (Depending on the RMX Manager configuration, you may have to click Rarely Used first.)
- **b** In the *IP Network Services* list pane, double-click **Management Network**.



The Management Network Properties dialog box is displayed.

- c Select the Secured Communication check box.
- d Click OK.

A message informs you that your session will be disconnected and that you must re-connect the *RMX* using **https** in the browser *URL*.

e Click OK.

A system restart confirmation message is displayed.

f Click Yes to restart the RMX.

The *RMX* restarts. System restart can take 5 - 10 minutes, depending on the *RMX*'s configuration.

- **g** In the *MCUs* list, select the *RMX* to be updated.
- **h** In *MCU Properties*, change the *Port* number from **80** to **443**.
- Click OK.

Appendix K - SIP RFC Support

SIP RFC Support in RealPresence Collaboration Server (RMX) Systems

SIP RFC	Description	Note
1321	MD5	
2032	RTP Payload for H.261	
2205	RSVP	
2327	Session Description Protocol (SDP)	
2429	RTP Payload for H.263+	
2833	RTP Payload for DTMF	
2617	HTTP Authentication	
2976	SIP Info Method	
3261	SIP	
3264	Offer/Answer Model	
3265	SIP Specific Event Notification	Limited support
3266	SDP Support for IPv6	
3311	SIP Update Method	
3515	SIP Refer Method	Limited support
3550	RTP	
3551	RTP Profile for Audio/Video	
3711	SRTP	
3890	Transport Independent Bandwidth Modifier for SDP	
3891	SIP Replaces header	Limited support
3892	SIP Referred-by Mechanism	Limited support
3984	RTP Payload format for H.264	
4028	Session Timers in SIP	
4145	TCP Media Transport in SDP	

SIP RFC	Description	Note
4566	Session Description Protocol (SDP)	
4568	SDP Security Descriptions	
4573	H.224 RTP Payload (FECC)	
4574	SDP Label Attribute	
4582	Binary Floor Control Protocol (BFCP)	
4583	SDP for BFCP	
4796	SDP Content Attribute	
5168	XML Schema for Media Control (Fast Update)	
cc-transfer	Call Transfer Capabilities in SIP	Limited support
draft-ice-19	ICE spec for firewall traversal in SIP	
draft-turn-07	TURN spec for firewall traversal in SIP	
draft-rfc3489bis-15	STUN spec for firewall traversal in SIP	

Appendix L - Homologation for Brazil

H.323 & SIP Protocol Flag Options

Using a set of system flags, the user has the ability to select either Polycom proprietary or H.323/SIP standard protocol settings.

H.323 & SIP Flag Settings

Three flags are enabled on the Collaboration Server, allowing the user to define and select either standard or proprietary H.323 and SIP protocol settings.

Flag name: SIP_TIMERS_SET_INDEX

Description: SIP Timer type timeout settings according to standard or proprietary protocol.

Flag section: CS_MODULE_PARAMETERS

Possible Values: either 0 or 1.

0 - Polycom standard (flag default setting)

1 - SIP Standard recommendation. For homologation and certification testing, this flag must be set to 1.

For use as a reference, the following table lists the SIP timer types for each flag setting and their corresponding timeout values in milliseconds.

SIP Timer Types

SIP TIMER Types	Value (in milliseconds)		
	POLYCOM (flag default)	Standard Recommended	
T1	50000	500	
T2	20000	4000	
TimerB	35000	32000	
TimerC	35000	60000	
TimerD	32000	32000	
TimerF	35000	32000	
TimerH	35000	32000	
Timerl	5000	5000	

SIP Timer Types

SIP TIMER Types	Value (in milliseconds)		
	POLYCOM (flag default) Standard Recommended		
TimerJ	32000	32000	
TimerK	5000	5000	

Flag name: H323_TIMERS_SET_INDEX

Flag description: Enables or disables H.323 index timer according to standard or proprietary H.323 protocol. Section CS_MODULE_PARAMETERS

Possible values:

- 0 Sets the H.323 index timer to Polycom proprietary (flag default setting)
- **1** Sets the H.323 index timer based on the H.323 Standard recommendation. For homologation and certification testing, this flag must be set to 1.

Flag name: DISABLE_DUMMY_REGISTRATION

Flag description: Enables or disables SIP dummy registration on the domain.

Flag Section: MCMS_PARAMETERS_USER

Possible values:

NO - Disables SIP dummy registration (flag default setting).

YES - Enables SIP dummy registration. For homologation and certification testing, the flag must be set to **YES**.